University of Nevada, Reno

Market Based Models for CYBersecurity information EXchange (CYBEX)

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Computer Science and Engineering

by

Deepak K. Tosh

Shamik Sengupta/Dissertation Advisor

August, 2016
We recommend that the dissertation prepared under our supervision by

DEEPAK K. TOSH

entitled

MARKET BASED MODELS FOR CYBERSECURITY INFORMATION EXCHANGE (CYBEX)

be accepted in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Shamik Sengupta, Ph.D. – Advisor

Murat Yuksel, Ph.D. – Committee Member

Mehmet H. Gunes, Ph.D. – Committee Member

Ming Li, Ph.D. – Committee Member

Sankar Mukhopadhyay, Ph.D. – Graduate School Representative

David Zeh, Ph.D. – Dean, Graduate School

August, 2016
Abstract

Rising rate of cyber criminal activities has caught the attention of everyone spanning industry, academia, federal institutions, and military agencies. The initiative to protect critical resources against future cyber attacks requires security investments complemented with a collaborative effort from every organization. Therefore, a robust CYBersecurity information EXchange (CYBEX) framework is required to facilitate Cyber-Threat Intelligence (CTI) sharing among the participants (firms) to abate the impact of cyber attacks.

Since many firms hesitate to participate in the sharing framework, we devise a CYBEX self-coexistence game that is aimed to guide the firms (players)\(^1\) to choose if they are interested to participate or not. The evolutionary analysis of the game results in a novel mechanism to enforce the firms toward participation by wisely varying the participation cost. Based on the derived conditional constraints from evolutionary analysis, we propose a dynamic cost adaptation algorithm for CYBEX where, participation cost is altered dynamically depending on the number of participants in the sharing system. We also formalize a distributed learning heuristic for the firms that helps them to attain evolutionary stable strategy (ESS) by learning from their previous action history.

After participating in CYBEX, rational players may opt differentiated sharing in the framework to gain economic advantage. To understand how the firms can be triggered to share more we formulate a game of information sharing where the firms potentially figure out how much of their CTI they want to share with the community of firms. Using evolutionary analysis, we derive the constraints under which different equilibrium strategies can be achieved and then derive the lower as well as upper bounds of incentives from CYBEX. The external incentives can be manipulated in an appropriate manner to motivate firms towards sharing all of their information\(^2\) truthfully with others.

\(^1\)The words “players”, “participants” and “firms” are used interchangeably throughout the dissertation unless they are explicitly mentioned otherwise.

\(^2\)The words “information”, “cyber-threat intelligence”, “cybersecurity information” are being used interchangeably throughout the dissertation unless it is explicitly mentioned otherwise.
Though working in a collaborative manner and exchanging security information with each other, corporations can proactively defend cybersecurity issues, without any incentives and possibility of information exploitation hinder the firms to share their breach/vulnerability information with the external agencies. Hence it is crucial to understand how the firms can be encouraged, so that they become self-enforced towards sharing their threat intelligence, which will not only increase their own payoff but also their peers’ too, creating a win-win situation. In this research, we study the incentives and costs behind such crucial information sharing and security investments made by the firms. Specifically, a non-cooperative game between $N$-firms is formulated to analyze the participating firms’ decisions about the information sharing and security investments. We analyze the probability of successful cyber attack using the famous dose-response immunity model. We design an incentive model for CYBEX, which can incentivize/punish the firms based on their sharing/free-riding nature in the framework. Using negative definite Hessian condition, we find the conditions under which the social optimal values of the coupled constraint tuple (security investment and sharing quantity) can be found, which will maximize the firms’ net payoff.

We also address the problem of cyber interdependency that is aggravated in a public cloud computing platform. Since the collaborative effort of organizations in developing a countermeasure for a cyber-breach reduces each firm’s cost of investment in cyber defense, cyber-threat information sharing among different organizations has the potential to maximize vulnerabilities discovery at a minimum cost. Using non-cooperative game theoretic analysis, we investigate to find optimal strategy of investment in vulnerability discovery and sharing their cyber-threat information, when multiple self-interested firms are operating on cloud domain.
Dedicated to,
My Family
and
My Advisor
Dr. Shamik Sengupta
Acknowledgements

First and foremost, I am wholeheartedly grateful to my advisor Dr. Shamik Sengupta who has been a great mentor, teacher, motivator, friend, and philosopher throughout my doctoral degree. It is him who has taught me perseverance, dedication, and eagerness to learn anything no matter how hard the things are. I am fortunate to have an advisor like him, whose endless supports lead me to reach such a beautiful destination, a Ph.D. degree. I will always be indebted to him throughout my life. Secondly, I would like to thank Dr. Murat Yuksel, Dr. Mehmet Gunes, Dr. Ming Li, and Dr. Sankar Mukhopadhyay for serving in my dissertation committee and providing very useful comments/suggestions to improve the thesis quality. I am sincerely thankful to Dr. Charles Kamhoua and Dr. Kevin Kwiat from U.S. Air Force Research Lab, Rome, NY, for the collaboration opportunity and help in directing my thesis toward a better angle.

I would like to thank all my colleagues from Computer Networking Laboratory (CNL) for constantly providing their emotional as well as intellectual support throughout my doctoral studies. I have thoroughly enjoyed working with them and I will miss their company. I also extend my gratitude to the Department of Computer Science and Engineering, UNR for their financial support and providing me an opportunity to serve as a teaching assistant.

I am deeply obliged and thankful to my masters thesis advisor Prof. Siba K. Udgata, who have been very inspirational and a great motivator over the years. Its him who encouraged me and gave me a strong base to pursue Ph.D. I cannot thank him more for his immense support and invaluable advices before and during my doctoral studies. I must thank my colleague/sister Dr. S. Mini for her moral support that helped me a lot to stay positive during my Ph.D. I thank her more for painstakingly reviewing this dissertation. Lastly, I thank my family and especially my elder brother Dr. Dilip K. Tosh for his unconditional support throughout my academic life. Without his vision and belief, I could not have made it to this far. I would also like to thank Prativa and my sweet little Angel for their constant love and affection. Finally, I again thank my advisor Dr. Shamik Sengupta for all his supports in completing my Ph.D. dissertation.
Contents

Abstract i

Acknowledgements iv

List of Tables viii

List of Figures ix

1 Introduction 1
1.1 Cyberspace and its Security ................................. 1
1.2 Cyber-Threat Intelligence (CTI) ............................. 5
1.3 Thesis Organization ....................................... 9

2 Background Studies 11
2.1 Information Sharing Standardization .......................... 12
2.1.1 Existing Solutions for Cyber-Threat Information Sharing 15
2.1.2 Standards for Structured Threat Representation .......... 23
2.1.2.1 Structured Threat Information Expression (STIX) 23
2.1.2.2 Cyber Observable eXpression (CybOX) .................. 25
2.1.2.3 Incident Object Description Format (IODEF) ........ 25
2.1.2.4 Common Attack Pattern Enumeration and Classifi-
    cation (CAPEC) .................................. 26
2.1.2.5 Vocabulary for Event Recording and Incident
    Sharing (VERIS) ................................... 28
2.1.2.6 Security Content Automation Protocol (SCAP) . 29
2.2 Ongoing Research Advancements ............................. 31
2.2.1 Economic Impacts of Vulnerability Disclosure .......... 31
### 5.1.3 Cost of Security Investment and Information Exchange  107

### 5.2 Optimization Problem  109
- **5.2.1 Best Response Analysis**  110

### 5.3 Results and Discussion  112

### 5.4 Summary  119

### 6 Cyber-Investment and Cyber-Information Exchange Decision Modeling  120

#### 6.1 System Model  121
- **6.1.1 Game Formulation**  121
- **6.1.2 Utility Formulation**  122
  - **6.1.2.1 Sharing and Investment Gain**  123
  - **6.1.2.2 Cost Components Modeling**  125
- **6.1.3 Modeling $p_i$**  125
- **6.1.4 Modeling Reputation Cost ($\zeta(l_i)$)**  127
- **6.1.5 Optimization Problem**  128

#### 6.2 Game Analysis  129
- **6.2.1 Existence of Nash Equilibrium**  129
- **6.2.2 Guidance for CYBEX**  133

#### 6.3 Results and Discussion  134

#### 6.4 Summary  138

### 7 Cyber-Threat Information Sharing in Cloud Platform  139

#### 7.1 System Model  140

#### 7.2 Game Model  141

#### 7.3 Game Analysis  147

#### 7.4 Numerical Results and Discussion  151

#### 7.5 Summary  157

### 8 Conclusions and Future Work  158
- **8.1 Future Work**  160

**Bibliography**  162
List of Tables

2.1 Cyber-Threat Intelligence Industrial Platforms . . . . . . . . . . . . . . . . . 13
3.1 Payoffs in Strategic-Form for Participation Game . . . . . . . . . . . . . . 54
4.1 Strategic-form of Information Sharing Game . . . . . . . . . . . . . . . . . . 92
7.1 Notations . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 144
7.2 Game in Normal Form . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 146
List of Figures

1.1 Target Distribution Chart [1] .............................................. 3
1.2 Exploitation of Internet by Cyber Thieves ............................. 4
1.3 Cyber attack kill-chain .......................................................... 7

2.1 Cybersecurity Information Sharing in Action ......................... 14
2.2 MISP Architecture [2] .......................................................... 16
2.3 CYBEX X.1500 Functional Blocks [3] ................................. 18
2.4 Various Sharing Architectures ................................................. 20
2.5 Sample scenario of TAXII message exchanges in a source/subscriber architecture ......................................................... 22
2.6 Relation between TAXII, STIX, CYBOX ............................. 26
2.7 IODEF Data Model .............................................................. 27
2.8 CYBEX Participation Architecture ........................................ 37
2.9 Architecture of sector-wide information sharing .................... 46

3.1 Population proportion variation under constraint (i) ............... 59
3.2 Population proportion variation under constraint (ii) ............. 60
3.3 Population proportion variation under constraint (iii) ............. 62
3.4 Population proportion variation under constraint (iv) ............. 62
3.5 Population preferred stable strategies based on conditional constraints ................................................................. 63
3.6 (a) Average utility growth, (b) Evolution of “Participate and Share” strategy population under different participation cost .......... 73
3.7 Evolution of average utility as the game progresses under different learning constant ......................................................... 75
3.8 Dynamics of “Participate and Sharing” Population under static and proposed dynamic participation cost ........................ 76
3.9 CYBEX’s gross revenue comparison under static and proposed dynamic participation cost charged by CYBEX ......................... 77
3.10 Evolution of participating population at different participation cost, when initial participant proportion is 0.65 ..................... 79
3.11 Evolution of participating population at different sharing cost, when initial participant proportion is 0.4
3.12 Evolution of participating population w.r.t. participation and sharing cost, when initial participant proportion is 0.65
3.13 Evolution of participating population at different sharing cost, when initial participant proportion is 0.4
4.1 Evolution of population demonstrating “No Participation” strategy as ESS
4.2 Evolution of population demonstrating “Low Sharing (LS)” strategy as ESS
4.3 Evolution of population demonstrating “High Sharing (HS)” strategy as ESS
5.1 Optimal Investment on own sharing level variation ($N = 2$)
5.2 Optimal Investment on own sharing level variation ($N = 20$)
5.3 Effect of others’ sharing level on Firm i’s investment
5.4 Utility vs. Number of participating firms
5.5 Effect of Firm i’s sharing level on received utility w.r.t. own investment level variation ($N = 4$)
5.6 Effect of Firm i’s sharing level on received utility w.r.t. other firms’ investment level variation ($N = 4$)
5.7 Effect of Firm i’s sharing level on received utility w.r.t. other firms’ investment level variation ($N = 20$)
6.1 Payoff comparison of greedy vs sharing nature
6.2 (a) Existence of Socially-Optimal Investment ($I^*_i$), (b) Existence of Socially-Optimal sharing ($l^*_i$)
6.3 Net utility vs. Sharing at different investment
6.4 Net utility variation at simultaneous optimization of Investment ($I_i$) and amount of information shared ($l_i$)
7.1 System Model
7.2 Venn Diagram Illustration of Discovered Vulnerability
7.3 Hypervisor Compromise probability vs. damage cost
7.4 Hypervisor Compromise probability vs. vulnerability discovery probability
7.5 Probability that attacker compromises hypervisor vs. Damage caused
7.6 Cost of sharing vs. Cost of Investment
7.7 Payoff vs. Vulnerability discovery probability
Chapter 1

Introduction

1.1 Cyberspace and its Security

Cyberspace has become a major part of human lives ever since Internet technology dominated over every aspect starting from simple record keeping to space missions. According to “internetlivestats” [4] website, currently there are more than 3 billion cyberspace users, which is close to 40% of the world population. Thus, four out of ten individuals are connected with the cyberspace where his/her personal information resides and is used to provision differentiated services based on their requirements. Not only individuals, rather governments, industries around the globe have also been expanding their horizon in various directions by enabling services over the cyberspace. Thus it is acknowledged that efficient utilization of cyberspace and communication technology are the key ingredients for social empowerment and economic growth. Ample evidences can be found in the web about usefulness of digital communication in managing disaster situations, creating national revolution, researching about other planets
etc. The myriad services and applications on cyberspace not only operate on personal data of individuals but also information from various sectors such as government, finance, health, energy, transportation, education, defense, etc., which are the backbone of any nation’s development. Apparently, successful growth, high economy and development of any nation have a great contribution from the cyberspace, and information technology solutions.

However, securing the vast cyberspace from modern day attackers such as hackers, terrorists, skilled corporate raiders, vandals and voyeurs etc. has become a critical issue for all cyber consumers. A sample scenario of cyber criminal activity is shown in Fig. 1.2. This darker side of the cyberspace costs millions of dollars every year to compensate and recover from the cyber attacks. Recent examples include cyber attack on Home Depot [5] that lasted for five months, where a custom-made malware named “zero-days” in their payment system breached 56 million of credit and debit card information. Nonetheless, the top target for the cybercriminals is the retail industry where point-of-sell attacks successfully leaks the users’ personal information to the attackers. Not only retail market, cyber war has broadened its horizon to health-care, energy, financial sectors too. In 2014, string of breaches [6] were laid out on major retailers like Target Corp, Neiman Markus, Kmart, Staples, Sony, Home Depot etc. Multiple data breaches on nation’s largest bank in terms of assets, JP Morgan Chase & Co. [7], had affected millions of households and businesses. In 2015, data breach on Anthem and Primera Blue exposed nearly 90 million consumers’ health insurance/health records [8]. Cyber attack on telecom giant T-mobile’s vendor, Experian credit-services, had affected approximately 15 million customers [9]. Recently a cybergang successfully infiltrated into more than 30 global financial institutions’ payment system and stole a billion dollar a sophisticated
malware named “carbanak” [10]. The robbery was well planned and robbing each bank took between two to four months on average. The survey presented in [11] describes the most exploited vulnerabilities in hardware, software and network level along with various mitigation techniques. They also provide a brief overview on evolved attack patterns in the current emerging technologies like social media, cloud computing, smart phones communication etc.

At one hand, the scalability of cyberspace is attracting businesses to transform their supply chains, marketing strategies, business models and expand globally, whereas on the other side, highly crafted cyber attacks like distributed denial-of-service (DDoS) [12], advanced persistent threat (APT) [13], zero-day attacks [14] etc., aim to disrupt the sanity of cyberspace and steal proprietary information for further exploitation. Therefore, cybersecurity has been a buzz word since past couple of years that is designed to understand the in and out of diverse cyber attacks and develop countermeasures/defense strategies to preserve the vital components of information technologies, i.e. confidentiality, integrity, and
The importance of cybersecurity is now being realized both by government and private enterprises after massive cyber attacks across numerous sectors. Therefore, a significant amount of funds is being invested towards boosting cyber defense capabilities in nation-wide and efforts from research & academia are being made to improve the cybersecurity awareness of federal as well as private corporations. To foster the security awareness and understand the threat landscape, firms require the up-to-date information about attack incidents so that proactive measures can be taken to reduce the impact of cyber attacks. Since the intelligent attacker can tactfully modify the existing exploits and reuse for attacking multiple targets, the organizations must utilize the up-to-date cyber information to derive Cyber-Threat Intelligence (CTI) out of it, so that it would be easier to prevent similar cyber attacks that a firm has already seen.
1.2 Cyber-Threat Intelligence (CTI)

Cybersecurity is a broad term that encompasses various components to protect the privileged resources from cyber-exploitation. To enable an effective cybersecurity risk management standard, organizations must be capable of quickly identifying, mitigating, and managing the cyber risks in a timely manner. Cultivating such process requires an experienced team of threat analysts, information security professionals, and most importantly a diverse knowledge of threat landscape. This knowledge is referred to be the cyber-threat intelligence (CTI) that may come from various sources including online sharing communities, open-source forums, commercial sources etc. The organizations may collect information by themselves about the low-level threat indicators of compromise like IP addresses, email, malicious URLs, command and control domain names, malware hash values, attack patterns, geo-location information etc. However, inferring the high-level information and many important attributes of the cyber attacks, such as targeted resources of the attack, information about threat actors, methods and tools used, attack characteristics etc., may not be easily revealed from the self-collected intelligence. Analysis of Cyber-threat intelligence, collected from a large set of cyberspace consumers, can provide concrete information about various vulnerabilities, different malware families used in the course of attack, compromised end points, etc., which are crucial to understand and predict the cyber attacks.

The high profile cyber attacks, also known as “Advanced Persistent Threat” (APT), do not occur in the blink of an eye, rather they are the consequences of multi-year intrusion campaigns by well-resourced and trained adversaries. The intrusion kill-chain conceptualized by Lockheed Martin [15] best describes
the end-to-end process of a well-planned and targeted cyber attack. As it can be seen from Fig. 1.3, the exploit phase is the critical state, where the target gets compromised, however, there are crucial prior goals that need to be accomplished such as reconnaissance, weaponize, and deliver phase. The adversaries collect as much information by investigating the targets in reconnaissance phase. In weaponize stage, the attack tools such as malwares, trojanized files etc., are packaged for delivering and executing at the victim-side systems. Then delivery stage constitutes delivering the malicious package to the target machines by various social engineering techniques. Once the target falls into trap by executing the package, the exploit phase is succeeded. Hence the adversary can now use additional tools to control and execute own mission to extract as much intellectual properties for gaining financial advantage. Once everything goes in favor of the adversary, it tries to maintain the backdoors on the target for long-term benefits. The quicker a defender understands the kill-chain of the adversaries, the chances of defeating the crime is better. The defenders would most likely want to anticipate and if necessary, mitigate the threats proactively before their critical assets are exposed by staying a step ahead of adversaries in the kill-chain. Each stage of the kill-chain generates critical cyber information for the defenders. However, without sufficient cyber-threat intelligence, understanding adversary activities and developing appropriate proactive defense strategies would not be successful. So it is important for the organizations to share their threat data with other trusted enterprises, including government, health, financial, educational sectors etc.

Envisioning that the threat intelligence sharing can be instrumental for auditing the state of threat landscape and possibly help to predict major cyber attacks, U.S. senate has recently passed the bill “S.754-Cybersecurity Information Sharing Act (CISA) of 2015” [16]. The bill encourages private companies, businesses, federal
organizations to share cyber-threat information with one another, where sharing firms will be given liability protection from lawsuits related to data sharing. This is clearly a major step towards protecting the nation from future cyberwar.

Though there is no global information sharing framework developed yet to facilitate CTI exchange among enterprises, there are a few independent sharing communities exist where threat related information are exchanged in a commercialized manner like source/subscriber form where users subscribe to certain services to get feeds related to cybersecurity news. To facilitate such sharing framework, ITU-T (International Telecommunication Union-Telecommunication) took the initiative to adopt Cybersecurity Information Exchange (CYBEX) [3] to tighten cybersecurity and infrastructure protection. It is also being investigated by network and cybersecurity personnel, policy makers, governments and economists. The CYBEX framework aims to provide a service of structured information exchange about measurable security states of systems/devices together with incidents stemming from cyber attacks.
Chapter 1. Introduction

Several industries are focusing to develop platforms for threat intelligence management which aim to facilitate information sharing in an automated manner and utilize the information/data to generate actionable results so that various organizations can proactively tackle cyber attacks. Some recently developed industrial solutions include Facebook’s ThreatExchange, IBM’s X-Force Exchange, HP ThreatCentral, AlienVault OTX, Checkpoint Intellistore etc. Irrespective of all these efforts, firms still hesitate to participate and share their cyber-threat information with other organizations for various reasons: (1) open sharing of threat intelligence might not give competitive advantages in the market; (2) skeptical about the incident reporting process because it might create a channel to the competitors or malicious agents to violate trust and exploit the reporting firm using its own information; (3) shared information might reveal violations of federally controlled regulations, where the firms do not want to get involved; (4) budget constraints to invest for participating in such exchange frameworks to share and receive threat intelligence reports. However, the current practice of using isolated cybersecurity mechanisms can be highly expensive yet mostly ineffective against the ever-changing tactics of cyber attackers. Rather the firms’ participation in information exchange process may provide economic advantages in a long run, which requires several issues to be resolved so that firms will be motivated to join the sharing framework and share their threat data truthfully.

The basic assumption in CYBEX architecture is that the participating firms must be always cooperative and truthful with each other. However, in reality the firms compete with each other for better competitive advantages, revenue, market share, and stakeholders etc. In addition to that the market competition is very distributive in nature where rational firms never cooperate without any profit. In such scenario, motivating the firms to participate in the sharing
framework and share their proprietary cyber-threat information truthfully with others is a challenging task to achieve. Therefore, self-enforcement schemes for the firms to drive them towards participation are of high requirement to succeed in CYBEX framework. This will necessarily maximize the social welfare of both the participating firms as well as CYBEX. Since CYBEX is also considered as another rational player in the market, it also intends to maximize its profit by enforcing as many firms in the market to the sharing framework, so that the net sum of the participation costs can be maximum. Thus, from CYBEX’s point-of-view, it is critical to study how the participation cost can be smartly used to bring more participants to the sharing framework, eventually evolving to a win-win scenario. If the firms choose to share, the underlying challenge is to balance the amount of shared information and security investment so that the success probability of future cyber attack will be reduced. This underscores the following critical questions: (1) how much a firm should exchange out of its total discovered information? (2) what amount of investment will be sufficient in the presence of information exchange? (3) how CYBEX can motivate the firms by providing incentives (in a dynamic manner) yet make the sharing system self-sustained so that sharing is done directly rather than through external means?

1.3 Thesis Organization

The rest of this thesis is organized as follows. In Chapter 2, we present a detailed description of related researches in the field of cybersecurity information sharing and describe the current efforts from industry/government to develop sharing frameworks. As a progression to motivate corporation to participate in
Chapter 1. Introduction

the information exchange framework, we modeled a CYBEX self-coexistence
game in Chapter 3, where firms are looking for to decide whether they want
to participate and share or not. The formulated game is analyzed from the
evolutionary perspective and derive conditional constraints where evolutionary
equilibrium state can be achieved. In Chapter 4, we extended the participation
game to 3-strategy sharing game where firms have differentiated sharing na-
ture and based on which they get incentivized from CYBEX. We analyze the
game using evolutionary game concepts and derived various constraints on
incentives to achieve evolutionary equilibrium. Chapter 5, we have modeled
a non-cooperative game among firms to find out what optimal amount cyber-
security information sharing can maximize the firms’ net payoff through best
response analysis. In Chapter 6, we address the problem of quantifying the
amount of investment and information sharing, a firm would decide to maxi-
mize the net payoff. We formulate a non-cooperative game and analyze the Nash
equilibrium conditions by maximizing the coupled-constraint optimization prob-
lem. Chapter 7 extends the idea and applicability of threat information sharing
to cloud domain where multiple users share a common platform. Since the users
are interdependent on each other for securing themselves, we formulate a game
model among users to analyze whether a firm should make security investment
and share vulnerability information with other cloud tenants or not. Chapter 8
finally presents the conclusions and future researches that we plan to conduct as
an extension to this dissertation.
Chapter 2

Background Studies

The information security has been a major concern for the companies since businesses adopted the cyberspace as their medium for all sorts of business operations. To protect the critical assets from cyber-exploitation, corporations are required to invest resources in terms of both monetary as well as man power. However, timely information on incidents, vulnerabilities, threat signatures etc., may not be discovered from sole cybersecurity research. The emerging standard of cyber-threat intelligence sharing can complement the security investments made by the firms if they decide to take part in such sharing frameworks. This topic has gained significant attentions and is being investigated by government, policy makers, economists, non-profit organizations, industries, cybersecurity and network professionals with researches in this particular area still emerging [17][18][19]. Several attempts are being made from government as well as many non-profit organizations to make the cyber-threat information (CTI) sharing a reality.
Chapter 2. Background Studies

2.1 Information Sharing Standardization

Envisioning that the threat intelligence sharing can be instrumental for auditing the state of threat landscape and possibly help to predict major cyber attacks, U.S. senate has recently passed the bill “S.754-Cybersecurity Information Sharing Act (CISA) of 2015” [16]. The bill encourages private companies, businesses, federal organizations to share cyber-threat information with one another, where sharing firms will be given liability protection from lawsuits related to data sharing. This is clearly a major step towards protecting the nation from future cyberwar. Though there is not a global information sharing framework developed yet to facilitate CTI exchange among enterprises, there are a few independent sharing communities existing where threat related information are exchanged in a commercialized manner or source/subscriber form where users subscribe to certain services to get feeds related to cybersecurity news. To facilitate such sharing framework, ITU-T (International Telecommunication Union-Telecommunication) took the initiative to adopt Cybersecurity Information Exchange (CYBEX) [3] to tighten cybersecurity and infrastructure protection. It is also being investigated by network and cybersecurity personnel, policy makers, governments and economists. The CYBEX framework will provide a service of structured information exchange about measurable security states of systems/devices together with incidents stemming from cyber attacks. A sample process of information gathering and sharing is shown in Fig. 2.1, where a firm regularly collects the incident data from its own corporate network and from various other firms who are participating in the sharing framework. Keeping all the cybersecurity threat information in a structured manner, the firm continuously digs and mines the data to strengthen its security awareness.
<table>
<thead>
<tr>
<th><strong>CTI Platform</strong></th>
<th><strong>Primary Focus</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. IBM X-Force</td>
<td>CTI sharing, aggregate actionable intelligence, peer collaboration</td>
</tr>
<tr>
<td>2. Facebook ThreatExchange</td>
<td>Share threat data in a group of participants using a convenient, structured, and easy-to-use API</td>
</tr>
<tr>
<td>3. HP ThreatCentral</td>
<td>Share the aggregated threat content from public feeds, security vendors, community members</td>
</tr>
<tr>
<td>4. AlienVault OTX</td>
<td>Collect Indicators of Compromise (IoC), Push to subscribers to update their defenses automatically</td>
</tr>
<tr>
<td>5. ThreatCloud IntelliStore</td>
<td>Provides relevant/up-to-date threat intelligence feeds based upon industry, attack types and geography</td>
</tr>
<tr>
<td>6. ThreatConnect</td>
<td>Aggregate threat data across various sources, analyze and understand the data, and develop course of actions</td>
</tr>
<tr>
<td>7. Microsoft Interflow</td>
<td>STIX [20] based security and threat information exchange platform</td>
</tr>
<tr>
<td>8. ThreatStream</td>
<td>Real-time multi-source acquisition, trusted sharing community creation to collaborate and analyze</td>
</tr>
<tr>
<td>9. Soltra Edge</td>
<td>Automated data de-duplication, STIX and TAXII [21] based intelligence dissemination to users, devices, and communities</td>
</tr>
<tr>
<td>10. ThreatQuotient</td>
<td>Centralized dynamic repository to provide enriched threat indicators with flexible scoring engine, aggregated threat data visualization</td>
</tr>
<tr>
<td>11. BrightPoint Sentinel</td>
<td>Manage volumes of threat data, automatic threat detection and risk analysis, share threat intelligence</td>
</tr>
</tbody>
</table>

**TABLE 2.1: Cyber-Threat Intelligence Industrial Platforms**
Several industries are focusing to develop platforms for threat intelligence management that aims to facilitate information sharing in an automated manner and utilize the information/data to generate actionable results so that various organizations can pro-actively tackle cyber attacks. Some recently developed industrial solutions toward threat-intelligence management are listed in the Table 2.1. Irrespective of all these efforts, firms still hesitate to participate and share their cyber-threat information with other organizations for various reasons: (1) open sharing of threat intelligence might not give competitive advantages in the market; (2) skeptical about the incident reporting process because it might create a channel to the competitors or malicious agents to violate trust and exploit the reporting firm using its own information; (3) shared information might reveal violations of federally controlled regulations, where the firms do not want to get involved; (4) budget constraints to invest for participating in such exchange.
frameworks to share and receive threat intelligence reports. However, the current practice of using isolated cybersecurity mechanisms can be highly expensive yet mostly ineffective against the ever-changing tactics of cyber attackers. Rather the firms’ participation in information exchange process might provide economic advantages to themselves as well as other participants in a long run. From an organization’s perspective, the phenomena of “my detection becomes your prevention” and vice versa will be very applicable if the corresponding firms support threat information sharing. However, there are several research issues that need to be addressed so that organizations will not hesitate to come forward and contribute to the cybersecurity information sharing community. Several efforts are being made from industry and academia to automate the threat information sharing process, which we discuss in the following subsections.

### 2.1.1 Existing Solutions for Cyber-Threat Information Sharing

Though the researches on vulnerability assessment [22][23] and security information sharing have been there from the past decade, the nation is still facing an increasing amount of cyber criminal activities. Noticing the benefits of vulnerability information sharing, government initiated to develop security-based information sharing organizations (SB/ISOs) such as Computer Emergency Response Team (CERT) [24], Sector based Information Sharing Analytic Centers (ISACs) [25], InfraGard, etc. in the early 2000. The Homeland Security Act of 2002 also highlights the importance of information sharing which by itself do not address the importance of incentivization mechanisms to facilitate information exchange. The problems for insufficient participation in information exchange process could be: (1) absence of standard mechanism to exchange the discovered
information (2) insecure feeling of firms to participate in the framework due to the fear of reputation loss (3) inefficient incentive model to attract corporations for sharing information, (4) requirement of appropriate threat information transportation mechanism or frameworks. Several efforts are made in the past to automate the process of cyber-threat information sharing and we list some important frameworks/developments in the following.

2.1.1.1 Malware Information Sharing Platform (MISP)

With combination of trusted community members, malware related knowledge base, and web-based platform, MISP [2] is built for sharing technical characteristics of malware among the members without caring about the incident context.
This standard is developed initially to support NATO Computer Incident Response Capability Technical Center (NCIRCTC) missions. It is combined with a searchable repository or database with automatic import/export of data in various formats such as plain text, XML, JSON, CSV, OpenIOC, SNORT etc., as shown in Fig. 2.2. MISP mainly takes care of the malware samples, their technical information or Indicator of Compromise (IOC). MISP has expanded its usability by allowing integration with other cyber defense tools like intrusion detection systems (IDS), GFI Sandbox, Andiant’s IOC Finder etc. Since MISP database provides API access as well as interaction through user interface, the community users may use different instances of MISP, where the instances are interconnected with each other to maintain consistency. Various CERTs and government agencies such as NATO, Belgian Defense, Computer Incident Response Center Luxembourg (CIRCL) etc., use MISP to improve automated threat detection and responsiveness to targeted cybersecurity attacks.

2.1.1.2 X.1500 CYBEX

ITU-T had attempted to build an emerging standard, Cybersecurity Information Exchange Framework (CYBEX) X.1500 [3], which is aimed to provide a common global format and assured automated platform for exchanging cyber-threat intelligence. The CYBEX framework is mainly built upon five important functional blocks: Information Description, Information Discovery, Information Query, Information Assurance and Information Transport. Fig. 2.3 depicts the functional blocks along with their supported standards.

- The description block takes care of structuring the cyber information for the purpose of sharing with others. Based on various operation
domains, such as knowledge accumulation, incident handling, IT asset management etc., specific ontologies are defined by several institutions and CYBEX framework supports most of them. For example, (1) describing information in knowledge base, CYBEX introduced Common Attack Pattern Enumeration and Classification (CAPEC) [26][27], Common Vulnerabilities and Exposures (CVE) [28], Common Weakness Enumeration (CWE) [29], Malware Attribute Enumeration and Characterization (MAEC) [30]; (2) for accumulating countermeasure knowledge for cyber-risks, CYBEX adopts Common Vulnerability Scoring System (CVSS) [31], Open Vulnerability and Assessment Language (OVAL) [32], and eXtensible Configuration Checklist Description Format (XCCDF) [33]; (3) presenting and storing cyber-incidents in incident/warning database, CYBEX allowed Incident Object Description Exchange Format (IODEF) [34] X.pfoc, and Common Event Expression (CEE) [35].

- The discovery block is meant to discover cyber-threat information
and entities, which uses two paradigms: centralized and decentralized discovery. In centralized case, information providers maintain hierarchical registries to store cyber-information using object identifiers (OID) [36]. Users can access the central registries and find what they are looking for. However, the main disadvantage is that the users first need to know if a particular registry exists or not. Discovering information in distributed manner can be achieved using resource description framework (RDF) [37].

• **Query block** is mainly used to request and respond cyber related information from the framework. CYBEX introduced X.chirp for this purpose, which is an extended SQL form to provide reliable query transactions.

• **Assurance block** is designed to check the validity of the information transacted in the framework. This module is important from the perspective of providing assurance to CYBEX users that the cyber-information is genuine and authentic. To enable such service, CYBEX introduced X.evcert, X.eaa and ETSI TS 102042 V2.0.

• **The transportation block** mainly serves the purpose of exchanging cyber-threat intelligence with other users over networks. X.cybex-tp describes the details of transport protocols which is based on Blocks Extensible Exchange Protocol (BEEP) [38].

Note that, the point of CYBEX is to provide a framework for users, not limited to businesses, corporations, end-users, government etc., where they can look for cybersecurity solutions and access them over Internet in an automated way. However, sharing vulnerability information from end-users/businesses to the CYBEX framework in a voluntary manner is critical to achieve, since rational
firms may not be willing to give away their proprietary information for public benefit without any self-benefits. Encouraging the private corporations to share their cyber-threat data voluntarily without any fear of lawsuits, federal government promoted the cyber-information sharing and recently passed the Cybersecurity Information Sharing Act (CISA) [39][16] bill.

2.1.1.3 Trusted Automated eXchange of Indicator Information (TAXII)

For enabling cyber-threat information sharing across organizations and product/service boundaries, a community driven effort by MITRE Corporation led by DHS came up with TAXII [21][40] standard. This provides an automated platform to exchange actionable cyber-intelligence between trusted partners.
or communities for proactive cyber defense. An excerpt from TAXII white paper [40] mentions that “TAXII defines services and message exchanges that can be part of an automated sharing infrastructure, as well as makes possible a single set of services and clients that can be used to interact with multiple parties, allowing a single investment in infrastructure and procedures to apply to multiple sharing communities”. The goal of this framework is not to initiate information sharing behavior among organizations and it does not address the trust agreements, governance, or any non-technical aspects of information sharing. Rather TAXII focuses on offering situational awareness about emerging threats to the cyberspace users/organizations, by enabling cyber-intelligence sharing via a single, common set of tools.

The TAXII standard is flexible enough for use by CTI consumers, producers, cybersecurity professionals, developers across industry, government, and academia. This standard supports various threat sharing models such as peer-to-peer, source-subscriber, and hub and spoke architecture as shown in Fig. 2.4. In case of peer-to-peer architecture, threat information flows from one peer to another, where any number of organization can become threat information producer or consumer or both at the same time. Unlike multiple producers in peer-to-peer case, one organization acts as single source of cyber information in case of source-subscriber architecture and all others basically subscribe to the threat provisioning service of source to acquire the threat knowledge. Hence the information flow is unidirectional, i.e. source to subscribers. In hub and spoke model, one central organization acts as a clearinghouse (hub) through which all the information are shared. Thus, when a spoke needs to share anything with others, it first exchanges the information with hub, which forwards to all other spokes after performing optional filtration or data analysis.
Three major functional units of TAXII serving the most of technicalities are (1) TAXII Transfer Agent (TTA), (2) TAXII Message Handler (TMH), (3) TAXII Back-end. TTA provides the networking ability and serves sending/receiving of TAXII messages by communicating with other TTAs over network. The inbound/outbound TAXII message are handled by TMH which ensures their formatting according to one or more TAXII Message Binding Specifications. The back-end is responsible for various activities not limited to data storage, subscription management, access control decisions, filtering of content prior to dissemination etc. In a broad sense, TAXII supports various capabilities to provision information exchange among companies such as discovery, pull, and push messaging services. To enable discovery of TAXII services including network addresses and their supported bindings by the TAXII clients, the discovery module comes handy. This capability also lets the clients know about what other TAXII capabilities the producer might have to offer and the technical mechanisms in achieving
automated information exchange. Push/Pull messaging services are useful for the producer as well as the consumer to send/request data feeds. Producer uses push messaging to forward periodical threat information to the consumers whereas consumer can request to pull data from producer, thus allowing the consumer to control its data flow according to its own convenience. A sample messaging communication between a producer and consumer in source/subscriber sharing model is shown in Fig. 2.5.

2.1.2 Standards for Structured Threat Representation

2.1.2.1 Structured Threat Information Expression (STIX)

Measuring the effectiveness of Cyber-threat intelligence (CTI) requires a formalized way to portray the threat information gathered from the corporations. Therefore, appropriate ontology for representing the threat intelligence is necessary. MITRE Corporation had put a significant effort in support of Department of Homeland Security (DHS) to come up with a structured language, named Structured Threat Information Expression (STIX) [20], for the specification, capture, describe and characterization of cyber threat information. This standard is designed not only to represent the threat information but also improve consistency so that they can be shared across organizations, stored and analyzed efficiently to develop overall cyber situational awareness. At a higher level, the key constructs of the STIX language are the important parameters used to describe cyber attack events such as (1) observables: the stateful properties or measurable events in cyber operational domain, for e.g. file name/hash, registry key update, HTTP
requests etc. (2) Indicators: specific cyber observable pattern along with contextual information that describes behavior of interest in cybersecurity and are potentially mapped to related TTP augmented with other metadata like indicator sightings and impacts with various detection mechanisms, handling restrictions, course of actions, related campaigns etc., (3) incidents: the discrete instances of indicators discovered during the process of incident response investigation, (4) tactics, techniques and procedures (TTP): represent the adversary exhibited behaviors, resources leveraged, victim information, kill chain phase, source, targeted resource, intended effect in the course of attacks, (5) exploitable targets: the system vulnerabilities or network configuration weaknesses inside the corporation which can be targeted for exploitation by threat actors’ TTPs, (6) course of action: defines corrective measures that need to be taken for addressing cyber threats and preventive actions to mitigate the impacts of incidents, (7) campaigns: define the set of adversary intents along with related TTP, incidents, actions taken in response to the campaign, (8) threat actors.

For the implementation of STIX standard, XML schema has been used, which helps in provisioning a portable and structured mechanism to facilitate smooth interaction among the involved organizations. Considering the benefits of STIX, DHS has adopted it including TAXII to share threat information between Office of Cybersecurity and Communications (CS&C) and its private/government partners. Financial Services Information Sharing and Analysis Center (FS-ISAC) has also agreed to implement STIX for sharing threat knowledge among its members in financial sector [41].
2.1.2.2 Cyber Observable eXpression (CybOX)

Another community-driven solution, CybOX [42], is designed to describe and characterize the events with stateful properties that are observable in cyber domain. CybOX is intended to provide common platform for all cybersecurity use cases demanding the cyber observable instances for prior analysis. Representing the cyber observables using this common structured schematic mechanism would open the opportunity of sharing this information with other organizations, and help in detecting attacks *a priori* through analysis. CybOX is supported in various cybersecurity domains such as: malware characterization, operational event management, logging, threat assessment, cyber situational awareness, incident response, indicator sharing, digital forensics etc. For instance, CybOX can be used to represent state of OS, disks, network traffic, files, etc., thus all critical events happening in the interim of attack can be captured easily. Since observables are the critical components to understand the signs of security breaches, STIX standard has the flexibility to include CybOX document inside it. The relationship between TAXII, STIX, and CybOX is portrayed in Fig. 2.6.

2.1.2.3 Incident Object Description Format (IODEF)

Internet Engineering Task Force (IETF) developed a standard entitled IODEF [34] for defining data representation, that offers a standard model for exchanging information by Computer Security Incident Response Teams (CSIRTs) to enhance their operational capabilities. Incident information on networks, hosts, services; attack remedies, forensic evidences, action methodologies etc., are conveyed in IODEF using XML representation. IODEF benefited CSIRTs in various
ways: (1) it strictly increased the automation ability in processing the cyber data and hence analysts do not have to parse unstructured textual documents, (2) reduced efforts in normalizing redundant information perceived from different sources, (3) helped to build common inter-operable tools for handling incidents and analyzing them. For every real world entity in representing organizational incidents, IODEF data model defines the Incident class as shown in Fig. 2.7, which is an XML tag in the IODEF document. IODEF-Document class represents the top level class of the IODEF data model. Besides, various classes are defined to represent incidents and their related activities, affected organization’s contact information, references to Internet registries, attack impacts, action history, methods used by intruders, expected solutions from the security analysts etc.

2.1.2.4 Common Attack Pattern Enumeration and Classification (CAPEC)

To understand the attackers’ perspectives, various attack patterns and classification taxonomies need to be comprehended. Structuring the attack patterns
will liberate the developers to enhance security of software that are protected from potential vulnerabilities. CAPEC [27], maintained by MITRE, provides a formal list of common attack patterns that are categorized in a meaningful way to convey software designers/developers about possible vulnerabilities in their system and how to effectively address them. Some examples of attack pattern are: filter failure through buffer overflow, SQL injection, HTTP response splitting, session fixation, phishing, forced deadlock, cache poisoning, etc.

CAPEC provides the attack patterns in two different forms: (1) CAPEC List, and (2) CAPEC Schema. The list is nothing but the collection of all possible attack
patterns that have been documented so far, whereas the CAPEC Schema is more structured format of the CAPEC List using XML based representation. STIX’s key construct tactics, techniques, and procedures (TTP) uses the backbone of CAPEC, hence STIX supports CAPEC as extensible alternative for representing attacker’s TTP and defender’s course of action.

2.1.2.5 Vocabulary for Event Recording and Incident Sharing (VERIS)

A well-known metrics framework, Vocabulary for Event Recording and Incident Sharing (VERIS) [43], provides another alternative to describe security incidents in a structured and repeatable manner. It targets to collect qualitative cyber-information and share anonymously and responsibly with others. VERIS schema typically contains information about various aspects of incident narrative. The comprising sections of a VERIS document are: (1) Incident tracking, (2) Victim demographics, (3) Incident description, (4) Discovery and response, (5) Impact assessment.

In incident tracking section of VERIS document, general information about the incidents such as unique ID, source ID, confirmation, incident summary, related incidents, confidence etc. are presented. Victim demographics section mainly describes the affected organization, which may not be sufficient to identify it. The purpose of this section is to compare incident relationship among various types of institutions. Attributes under this section are type of industry, country of operation, state, number of employees, revenue, locations affected etc. Cyber-threat actors and their actions, affected resources and compromised security attributes etc. are mainly used to describe incidents in VERIS document. The discovery and response section describes the timeline of the incident such as how
and when the incident was discovered, duration of compromise, root causes, corrective measures, whether targeted or opportunistic attack, etc. In impact assessment section, the losses occurred to the organization are quantized through various attributes, for e.g. loss category and estimation, impact rating, currency etc. VERIS community allows the document to be shared and exported to other suitable schema like STIX. VERIS v1.3 is based on Java Script Object Notation (JSON) format. The project also provides an open and free repository, VERIS Community Database (VCDB) for publicly reported security incidents in VERIS format.

2.1.2.6 Security Content Automation Protocol (SCAP)

SCAP [44][45] is another effort from US National Institute of Standards and Technology (NIST), which is a suite of specifications for organizing, expressing, and measuring security information using standard reference data collected from flaws in software, security configuration etc. At enterprise level, manual verification of software installation, system security configurations, indication of compromise, installing patches, managing security at OS, application, network level etc. are tedious to conduct. Automating all these time-consuming processes, SCAP’s standardized methods come handy.

The technical specifications of SCAP are categorized into five groups:

1. **Languages** provide necessary vocabularies and conventions for defining security policies, specify and generate checklists, provide low-level testing procedures that checklists use. The included languages in SCAP are Extensible Configuration Checklist Description Format (XCCDF) [33], Open
Chapter 2. *Background Studies*

Vulnerability and Assessment Language (OVAL) [32], Open Checklist Interactive Language (OCIL). XCCDF is used to express security checklists/benchmarks, OVAL represents information about system configuration, machine state etc., OCIL language is used to express security related questions for users and interpret the answers too.

2. **Reporting Formats** define the constructs to describe the collected information in standardized format. Two specifications are (i) Asset Identification: express known identifiers and asset information, (ii) Asset Reporting Format (ARF): express transport format of asset information and relationship between assets and reports.

3. **Enumerations** provide standard naming format and an official dictionary to list items. The supported specifications are Common Platform Enumeration (CPE) [46], Common Configuration Enumeration (CCE) [47], and Common Vulnerabilities and Exposures (CVE) [28].

4. **Measurement and scoring systems** define necessary method to evaluate various characteristics of a security weakness. The supported specifications are Common Vulnerability Scoring System (CVSS) [31] and Common Configuration Scoring System (CCSS) [48].

5. **Integrity** specification helps to maintain the integrity of SCAP content and results. The supported specification to enable integrity is Trust Model for Security Automation Data (TMSAD) [49].
2.2 Ongoing Research Advancements

The information security has been a major concern for the companies since businesses adopted the cyberspace as their medium for all sorts of business operations. To protect the critical assets from cyber-exploitation, corporations are required to invest resources in terms of both monetary as well as manpower. However, timely information on incidents, vulnerabilities, threat signatures etc., may not be discovered from sole cybersecurity research. The emerging standard of cyber-threat intelligence sharing can complement the security investments made by the firms if they decide to take part in such sharing frameworks. This topic has gained significant attention and is being investigated by government, policy makers, economists, non-profit organizations, industries, cybersecurity and network professionals. The research in this particular area is still emerging. As described in the earlier section, several attempts are being made from government as well as many non-profit organizations to make the cyber-threat information (CTI) sharing a reality.

2.2.1 Economic Impacts of Vulnerability Disclosure

Ideally, no software system is completely bug-free and discovering every vulnerability in the system is difficult to achieve. However, from the security standpoint, it is important for the organizations to discover and fix the vulnerabilities so that they can protect themselves from cyber exploitation. Considering a market scenario where CERT acts as an information distribution hub (infomediary) between the benign vulnerability identifiers and software users, [50][51] studies whether monetary reward to the vulnerability reporters would lead to improve social
outcome or decrease it. Since this incentive might attract attackers to discover vulnerabilities, it can decrease the social welfare as the number of discovered vulnerabilities by attackers grow. The authors formulate a two-period game with assumption of single vulnerability exists in the product, and the decision parameters such as incentive to the identifier for each reported vulnerability, subscription fee are controlled by the infomediary. The total industry loss and total user loss are computed to measure the welfare-metrics for both regulated market, where infomediary only cares about non-subscribers and non-regulated market, where the infomediary is assumed to be greedy.

Though some identifiers disclose the vulnerabilities in public forum to force the vendors to release early patches [52], this may be beneficial for attackers to utilize these vulnerability information for exploitation. Thus, attack frequency clearly depends on the status of vulnerability and corresponding patch disclosures. Authors of [53] empirically analyze that impact of disclosures and conclude that attack frequency is higher for patched vulnerabilities compared to the non-published and published but not patched vulnerabilities. This is possible because of the assumption that patches could be accessed openly by any third-party agents, which may not be the case anymore. To minimize the social loss and impact of cyber attacks, appropriate vulnerability disclosure mechanisms (e.g. full vendor, immediate public, and hybrid) need to be chosen. Authors of [54] mention that choosing optimal disclosure mechanism depends on several factors such as risks associated with the vulnerability, vendor’s incentive to develop patch, cost structure of software users etc. Minimizing the societal loss of vulnerable firms, and patch development cost of vendors, optimal patch-release policy (when to release and amount of time required) is decided. Patch-release
and patch-update policy of vendor and firms respectively is studied in [55] by considering both centralized (decided by a coordinator) and decentralized way.

### 2.2.2 Investment and Information Exchange Decision

Securing critical assets of an organization demands investment in terms of time, money and human resources. An increased level of security can be achieved through exchanging threat-related information with peer firms, government security organization etc. [18][56] provides necessary and sufficient conditions to verify this fact that optimal information security can be attained at a lesser cost provided security information is shared. Since firms share their threat data, some firms might take the opportunity to free-ride without exchanging anything back. Thus appropriate incentivization mechanism is required to prohibit the free-riding on other firms’ security information so that no firm can gain more by making under-investment. As the under-investment can bring serious cyber issues, [57] constructed a game theoretic model to address economic motivation of security investment and mentions the challenges of regulatory scheme design that mandates specific security standards. Though it is known that security investment is a mandatory requirement for the organizations to maintain information security, it is vital to come up with sophisticated cost-benefit methods to derive right amount of investment to make in cybersecurity. Gordon-Leob model [58] emphasizes in determining the optimal level of investment by taking the potential loss and severity of vulnerability into consideration and this model is well-accepted in the research community.

Cyber attacks in real can be categorized into two types: targeted and opportunistic, which may have different impact to the affected firms. Thus it is not wise
to make uniform security investments without knowing the characteristics of the attack. [59] studies investment decisions on such scenarios under various use cases by varying firm’s intrinsic vulnerability parameter, potential losses from breach, and attack probability due to firms’ interdependency. The interdependency plays an important role in cloud domain, where virtual machines (VMs) share a common platform. Thus possibility of side-channel attacks can make other resident firms vulnerable to cyber attacks. [60][61] study the decision of security investment and information sharing with other VMs by modeling the problems as non-cooperative games. As the socio-economic loss of a firm depends on the nature of information that is being shared with others, which has not been addressed in [18], Campbell et al. and Goel et al. in [19][62] analyze the market reaction of firms’ in terms of their stock value depending on the involvement of confidential information in the disclosed breaches. It is reported that cyber attacks that are related to unauthorized access to confidential data draw a significant negative market reaction.

The quest of finding optimal amount of expenditure [63] and information to exchange with others for strengthening a firm’s security gained its importance and many researchers looked into this problem by considering a social planner in the system who can help firms in deciding the mentioned decision parameters so that their social welfare is improved. Using game theory, authors of [64] investigate the competitive implications of information sharing and security investment and showed that benefit of this sharing is contingent on product substitutability. They also analyzed the consequences of establishing information sharing analytic centers (ISAC) that will help in coordinating the information sharing process without allowing free-riding. However, the social outcome of every participating firms is dependent on the extent firms’ rely on the social
planner’s decision. Hausken in [65] also addressed the similar problem by proposing a simultaneous and a two-stage game in the presence of an attacker but considered a new parameter called interdependency between the firms to analyze how this factor affects the social outcome of each firm. He showed that the two-stage game helps the firms to achieve higher outcome compared to simultaneous game, because the social planner cannot impose its decision on the firms when the interaction is simultaneous in nature.

Cavusoglu et al. proposed a similar game theoretic model in [66] like Gordon et al. [58] to determine the IT security investment levels and compared it with a decision theoretic approach on various dimensions such as vulnerability, payoff from investment etc. They also provide a learning model for the firms to estimate the hacker’s effort and utilize this value to accurately determine the optimal investment level. As the past works do not consider any specific type of information to share and the range of information sharing amount varies between 0 to 1, authors of [67] adopt a 2-stage Bayesian game considering the information as the number of bugs and using backward induction they derive the optimal investment quantity and number of bugs to share with the other firm. They also provide a mechanism to encourage other participating firms to share more information so that social inefficiency can be avoided and win-win situation can be brought in. Since most of the research works implicitly assume that firms share their information voluntarily among each other, this may not be always feasible due to organizational or privacy policy. Following the mandatory information sharing between firms and authorities, [68] devises a principal-agent model [69] to derive socially optimal value of security investment and amount of security breach reporting. Penalties are applied when the principal finds that the agents do not report their breach information in the course of random security audits.
Categorizing the information as substitutable and complementary with respect to other firm’s information, Liu et al. studied the implications of knowledge sharing and security investment decisions of two firms in [70]. It is found that the firms are naturally inclined to share if the information are complementary by nature, however, the firms invest sub-optimally. In case of substitutable information, the firms prefer not to share due to prisoner’s dilemma like conflict situation and therefore requires involvement of external agent like social planner. Since many research works introduce the breach probability function (BPF) as the important parameter for investigating information security, [71] employs a widely accepted BPF and analyzed efficiency of security investment and information sharing under the effect of breach probability. They analyze and compare a few other parameters at equilibrium such as aggregate attack, aggregate defense and breach probability with centralized decision cases those involve social planner. It is found that intervention of social planner increases the social outcome of the firms, and they argue that information sharing is independent of efficiency of security investment.

Involvement of social planner does not keep human out of the loop in deciding firms’ crucial private parameters such as amount of investment to make, amount of information to share etc. Hence, distributed incentivization schemes are very required to successfully automate the cybersecurity information exchange process, where firms can take decisions independently. Considering CYBEX as an authority that acts as central hub of information exchange process, a simultaneous non-cooperative game among the information-seeking firms is formulated in [72][73] to decide the amount of cyber investment to make and amount of information to share with other participants via CYBEX. CYBEX dynamically incentivizes the players based on their contribution to the sharing
community so as to self-enforce the participants to share truthfully and avoid the free-riders. In the above work, it is inherently assumed that the players or firms are participating in the information sharing process or CYBEX, which is another decision (whether to join or not) that the firms need to take. To model such participation scenario, [74] formulates an evolutionary game and analyzes it to find various conditions under which CYBEX can dynamically vary the participation cost to self-enforce the firms to participate in CYBEX as depicted in the Fig 2.8. A distributed learning heuristic is also proposed to let the firms achieve the evolutionary stable strategy (ESS).

![CYBEX Participation Architecture](image)

**Figure 2.8:** CYBEX Participation Architecture

### 2.2.3 Modeling Cyber-Threat Information Sharing

Since cyber-threat intelligence plays a major role in understanding the security landscape, some recent researches come forward with designs of threat intelligence management systems. [75] designs a system to share the threat intelligence along with course of actions (CoAs) in the form of a STIX document. The goal of the threat response management system is to process the collected threat information from various sources or providers and generate a report that
recommends the necessary CoAs. To facilitate communication between threat information providers for data acquisition, they leverage Extensible Messaging and Presence Protocol (XMPP) [76] queries and publish-subscriber protocols. With such messaging framework, the system enables various management operations such as dynamic discovery of threat intelligence providers, authentication and authorization services, secure way of communication among various entities.

Using extensive set of attributes in STIX, [77] proposes a sharing infrastructure to exchange information between two distinct parties such as: (1) Computer Security Incident Response Teams (CSIRT) at public and private organizations, (2) Security Intelligence and Coordination Centre (SICC), which acts as the hub of Hub and Spoke sharing model and it produces, collects and shares cyber threat intelligence with various CSIRT. To describe the threat incidents, the authors describe various meaningful impacts, the corresponding tag in STIX document, and the possible values for these attributes.

Lack of global large-scale information sharing platform which can provide accurate, consistent and high quality threat data motivate the current cybersecurity engineers as well as researchers to come up with a flexible sharing framework that will enable efficient collaboration among organization. A Cyber Security Data Exchange and Collaboration Infrastructure (CDXI) [78] is developed at NATO Communications and Information Agency to develop a sharing platform that satisfies the above mentioned criterion. The high level requirements of CDXI is concisely described in [78]. With similar requirements, [79] proposes a group-centric collaborative information sharing framework to improve community effort toward cybersecurity. Extending the group-centric Secure Information Sharing (g-SIS) framework [80], which supports information flow in the isolated groups but not between groups, the authors of [79] build the formal
model of collaborative information sharing framework by including inter-group relationships among various groups.

For establishing national cyber situational awareness, [81] designs a conceptual framework for Cyber Attack Information System (CAIS) and realizes the cyber-incident response cycle for both CAIS stakeholders and national cyber defense center. The CAIS stakeholders are none other than various organizations like banks, utility providers, IT vendors, network operators etc., that are primarily responsible for managing their critical assets and infrastructure, detect network anomalies, and report local incidents to national cyber defense center. On the other hand, the defense center undertakes the task of collection, aggregation, and evaluation of the reports submitted by the subscribed organizations and is responsible for providing policy based advices/recommendations to establish situational awareness. The above proposed architecture has some similarity with X.1500: CYBEX standard. However, the key challenges in developing threat management platforms as posed in [82][83] are still unresolved.

### 2.3 Emerging Challenges

This area of research has still a long way to go before reaching the ultimate goal of information sharing in a fully distributed environment without seeking help from any external agent. There are still many unanswered questions that an information exchange framework must resolve before adopting any particular idea. Some of those questions are: (1) how to design and analyze various self-enforcing incentive mechanisms when there are more than two firms willing to participate in the framework? (2) Can cyber-insurance be used as a potential
parameter that motivate and maximize the information sharing activity within the framework? (3) What conditions on cyber-insurance can help in achieving evolutionarily stable situation of maximum participation and maximum sharing in the system? (4) How can we devise a decentralized learning in the sharing framework that will help the individual agents to learn independently about the sharing attitude of its opponents and accordingly adapt their information sharing nature?

Nonetheless, the following key problems also add onto the stack of above discussed issues, which are crucial to be resolved by the researchers before the nation can adopt any standard framework for cyber-threat information exchange.

### 2.3.1 Policy and Legal Issues

The critical impediment to cyber-information sharing can be the liability to the laws regulating business operations and handling personal identifiable information (PII). Though CISA act ensures that private sectors can share their cybersecurity threat data with DHS or other federal agencies, “not withstanding any other provision of law”, it is mandatory that the information receiving organizations must not have conflict data handling regulations, which may occur in scenarios of threat information sharing in a global scale. Without appropriate information exchange policy, it will be difficult to figure out the originator of the received data and hence the receiving organization may not completely rely on it.

The other issue that may arise is information privacy disruption. Though organizations share their threat intelligence with either to an analytic center (referred as
hub in hub-spoke sharing model) or to a peer (in peer-to-peer sharing model), the inherent assumption is that the information originator should not get exploited using its own threat intelligence. The presence of malicious organizations or vicious attackers in the sharing community may target other participating firms or alter the integrity of the shared information, which must be prohibited through appropriate policy design. As information sharing framework is envisioned to be applicable on a global scale where national boundaries are no longer a limitation, it is important to maintain clear policy for international information exchange. Distinct national policy on packet analysis may hamper the sanctity of shared information and eventually it may not be of much help to address cybersecurity issues. Hence, the international information exchange agreement will help in deciding several important attributes regarding the sharing process such as: format of exchange (whether free text or structured document like STIX, VERIS, SCAP etc.), restrictions on packet content, size limitation of data exchange, certificate to authenticate data, specifics of communication mechanism, information quality requirement etc.

organizations would have to deal with the information content received from unfamiliar organizations (possibly malicious entities), it is vital to have strong preprocessing techniques to discard the inconsistent, erroneous, and redundant cyber data. To not fall on the trap of privacy disruption, organizations must use de-identification methods to remove PII from the indicator information to share before the content leaves the corporate boundary. Also some firms require to perform cost-benefit analysis to weigh whether it is worth to participate in the sharing framework and perform all tasks to retrieve intelligence from the received threat data.
To generate useful insights and develop remediation strategies from cyber data, the organizations not only require information from other corporations but also need data from their own network, computers/servers etc. Thus the corporations require a generic ecosystem that can integrate cyber-intelligence from others and own network operation data seamlessly to derive better, faster and actionable security measures to prevent cyber-criminals trespassing the corporate boundary. Given a large volume of data, the organizations need to mine the data to derive actionable intelligence out of it, which is a challenging task.

2.3.2 Ontological Issues

As the field of cybersecurity has evolved to a great extent in the past half decade, significant efforts are being made from both industry and academia to devise formal schemes to represent cyber threats and their impacts. Though there are several standards, for e.g. STIX, VERIS, SCAP, CybOX, OpenIOC etc., developed by various organizations to represent threat information, different firms might adopt different terminologies and language standards according to their convenience. Hence, this will create extra hassle for the firms in interpreting the collected information since the ontology used by different firms are different. It is challenging to build automated tools to adapt the ever evolving cybersecurity standards. The most popular STIX standard has already more than eight versions in past three years, which hints that corporations may face the issue of standard mismatch and may miss the semantics of exchanged information.
2.3.3 Information Relevancy

Relevancy of shared data is an important metric to measure the data quality. Organizations investigating on their security aspects may produce threat data that are unique and relevant to its own nature of operation, application environment, operating systems used, etc. However, these conditions might not be same for other consumer firms, and thus every piece of threat information from the former firm may not be applicable to consumer firms. For an example, threat data corresponding to a Linux operating system may not be precisely useful for a firm that uses windows OS. Thus, heterogeneity in organizations’ technologies/applications might have an impact on their information sharing and consuming behavior. Considering the ideal information sharing relationship among organizations should last forever, irrelevancy and heterogeneity of threat data may demoralize the firms from sharing. Without relevant threat intelligence in return, the organizations have no incentive to share their own information.

It is also important to determine the relevancy of received data periodically, which will help the firm to build a trust relationship with the source organization. It is natural to see that the firms sharing relevant threat intelligence can be relied more as long as the same behavior sustains, whereas it is hard to trust someone that shares inconsistent or irrelevant threat data. There can be many relevancy determination criterion, such as (1) credibility/reliability of data source, (2) potential impacts on organization’s cybersecurity issues (3) quality of threat-intelligence resulted, (4) attack frequency after information exchange, etc.
2.3.4 Privacy Protection

Cybersecurity information sharing implicitly brings the privacy risks of exposing personal identifiable information (PII) or any organizational sensitive data. Thus firms require appropriate actions to balance the privacy concerns and control the process of cyber data dissemination. The topic of protecting privacy and confidentiality of cyber data has been a subject of interest for policy makers and cybersecurity professionals. Some observers argue that cyber incident report does not require privacy-related information and hence it is easy to exclude all the PII from threat data before sharing using anonymization techniques. However, it is counter-argued that the high profile data mining and data analytic techniques have capabilities of deriving private information of the contributor. Thus it is important to investigate the potential risks targeting the privacy and confidentiality of public/private sector organizations involved in the information sharing activities.

2.3.5 Motivating Firms for Information Sharing

The basic assumption in CYBEX architecture is that the participating firms must be always cooperative and truthful with each other, which may not be feasible always. In reality the firms compete with each other for better competitive advantages, revenue, market share, and stakeholders etc. In addition to that the market competition is very distributive in nature where rational firms never cooperate without any profit. In such scenario, motivating the firms to participate in the sharing framework and share their proprietary cyber-threat information truthfully with others is a challenging task to achieve. Therefore, self-enforcement
schemes for the firms to drive them towards participation are of high requirement to succeed in the sharing framework like CYBEX. This will necessarily maximize the social welfare of both the participating firms as well as the sharing framework. Since it is inherent to assume that CYBEX model is another rational player in the market, it also intends to maximize its profit by enforcing as many firms in the market to the sharing framework, so that the net sum of the participation costs can be maximized. Thus, from CYBEX’s point-of-view, it is critical to study how the participation cost can be smartly used to bring more participants to the sharing framework, eventually evolving to a win-win scenario. If the firms choose to share, the underlying challenge is to balance the amount of shared information and security investment so that the success probability of future cyber attack will be reduced. This underscores the following critical questions: (1) how much a firm should exchange out of its total discovered information? (2) what amount of investment will be sufficient in the presence of information exchange? (3) how CYBEX can motivate the firms by providing incentives (in a dynamic manner) yet make the sharing system self-sustained so that sharing is done directly rather than through external means?

2.3.6 Sector-wide Information

Every corporation has its own business to handle, which can be categorized to financial, information technology, energy, healthcare, transportation, defense/military, educational, retail domains etc. The cybersecurity information generated by a firm which belongs to a particular sector may not be useful to another firm belonging to a different sector as portrayed in Fig. 2.9. Based on the nature of cybersecurity information, it is necessary to understand whether firms
would prefer to share all of their discovered information with a specific set of organizations based on their trust relationship. Sector-wide biasness may lead to a market segmentation of cyber-threat information. However, absence of collaboration from different sectors may not enable global situational awareness even though such topology reduces the density of information flow. Another important challenge arises when the firms share their information with firms of same sector but they may act untruthfully to gain competitive advantages. In such scenario, it would be critical to detect the free-riding firms and necessarily penalize them to prevent such action in future.

2.4 Summary

While cyberspace has brought enormous advantages for corporations and individuals, it has also created a channel for the cyber criminals to steal intellectual properties of cyberspace users. Past years have seen enough evidences about
what sort of havoc the cyber attackers can create. Thus, it is of utmost important for every entity, including federal agencies, private corporations, network professionals, policy makers etc., to address the issues of cybersecurity by any means so that the nation can stay protected from any critical hazard. A collaborative effort from private organizations and federal firms is highly required, where every individual firm should share its vulnerability information with others. This will not only help in developing awareness on cyber threat landscape, but also create a large intelligence base that can be used to derive actionable information to pro-actively defend cyber attacks. In this Chapter, we have studied the necessity and importance of cyber-threat information sharing in practice and present the recent developments in terms of industrial solutions and academic researches. With considerable amount of effort in building information sharing platforms, there are still a handful number of issues existing and need to be resolved before the community can adopt the right solution. We, therefore, address a few open research challenges that have a great impact in motivating the firms to voluntarily participate and share their threat intelligence in the next chapters of this dissertation.
Chapter 3

Self-Coexistence of Firms in CYBEX Framework

3.1 CYBEX Participation Game

Though the corporations or firms understand the benefits and costs of cyber-threat information sharing, not everyone of them takes the risk of participating in CYBEX framework. Thus, motivating the firms to participate in the exchange framework and guiding them toward a self-sustained framework are some of the critical issues to address from the CYBEX’s point-of-view. We aim to present a self-enforcement mechanism that will attract firms to participate in the sharing framework which can maximize the net benefit of participants while increasing the proportion of firms in the framework. From the perspective of CYBEX, charging a cost for participation will maximize its net revenue only if the number of participants is maximized. This might be difficult to achieve without adopting a scheme for dynamic participation cost. To analyze such scenarios, we
model the CYBEX participation game and analyze it using evolutionary game dynamics.

3.1.1 Game Model

In this work, we consider the generic abstraction of “always rational and profit-seeking” CYBEX and firms. We consider a market scenario, where there are $N$ firms playing independently in this game and trying to decide whether to participate in the CYBEX framework and share with other firms by incurring a participation cost. From CYBEX point-of-view, the decision problem is how much incentive/participation costs should be induced and when, to motivate the firms to participate in the CYBEX framework. If CYBEX charges too high to increase its revenue, the firms may possibly get deterred from participation, eventually reducing CYBEX’s revenue. On the other hand, if CYBEX charges too low to attract firms, the revenue generated by CYBEX might be insufficient to sustain in the market. Thus it is important to investigate, under what conditions and how CYBEX can dynamically decide on incentive/participation cost to attract increasing number of participants to share (which will increasingly strengthen their cyber-defense capability), yet increase CYBEX’s revenue. To model the firms’ payoff, the following two components are considered here.

3.1.2 Sharing and Investment Gain

In this evolutionary information exchange framework, assuming the firms invest for their own cybersecurity R&D, the firm directly benefits from its own investment. Additionally, an indirect reflected gain is received from the other firms’
shared information, which can produce proactive defense, patches and fixes. Therefore, exchange of this valuable information with other firms improves their overall utility. Though participating in CYBEX and sharing information is beneficial for protecting the firms’ assets from cyber criminal activities, the participation in the CYBEX architecture and sharing information among the firms are not cost-free.

3.1.3 Modeling Costs in CYBEX

There exists a cost of participation in the CYBEX architecture, which is defined by the cost that the CYBEX architecture charges the firms for maintenance of the architecture as well as certification (for sharing) and to ensure liability of the firms. Apart from the participation cost, there also exists a cost of information sharing, which has two parts: retrieving the information for relevance, and the potential loss of reputation. Therefore, self-enforcement schemes need to be devised to motivate and attract the firms to participate and share in CYBEX framework.

3.2 Motivations of using Evolutionary Game Approach

The motivations of opting evolutionary games to model firms’ participation and information sharing decision comes from the nature/quality of strategies (solutions) obtainable from the evolution process of the players in such games. Especially, the rational organizations would continuously evolve in real time until every player adopts to a stable steady-state strategy. In the process, the fitter
strategies get prevalent and the unfit ones become extinct over time. To model such situations, evolutionary games come handy that are useful to understand the stability of strategies over a finite population of players. Hence, any game can be analyzed using evolutionary concepts to find the stable strategies irrespective of number of players in the system [85]. However, stability of strategies may not be understood from non-cooperative game solutions.

As far as non-cooperative game models are concerned, they are widely used to model problems where, players of the game make their decisions independently without any sort of help from the competitors. The outcomes of these games are the equilibrium strategies with respect to other players’ actions. However, evolutionary games extend the idea of non-cooperative games by introducing a population of agents (a group of players), who are interacting with each other dynamically and evolving to figure out the fittest strategies that could help them to survive in the game while the unfit players’ strategies get invaded over time. Such games are highly applicable when the individuals exhibit different behaviors at different times and posses the ability to evolve over time for their betterment. The interaction of a player with a group of players exhibiting different behaviors may give him/her a scope for evolution, which can eventually lead to adopt a stable strategy. Thus, it is important to understand the dynamics behind such group interactions, which cannot be measured effectively in isolation. Rather it has to be evaluated in the context of entire population where the player lives.

Additionally, the following characteristics of evolutionary games [86][87][88] motivated us to model our problem accordingly in this research.
1. **Equilibrium Solution Refinement**: The evolutionary games always provide a refined solution that ensures stability of a strategy adopted by a population, where *no small subgroup of deviants could successfully invade the whole population*. Such strategy is known as evolutionary stable strategy (ESS). However, in case of non-cooperative games, Nash equilibrium (NE) is considered as the traditional solution concept, which by definition ensures that no player can gain more by deviating unilaterally to a different strategy [89]. But if a group of players collaboratively change their strategies simultaneously instead of adopting NE, then they may increase their net payoffs [90] and this importantly differentiates ESS from NE solutions. If both of the solutions are compared, outcomes of evolutionary games are stronger and efficient than the outcomes of a non-cooperative games. In general, ESS are nothing but the refined subset of NE strategies, that provides no lesser payoff than a NE strategy [85][91], if opted.

2. **Bounded Rationality**: In traditional game theory, the individuals are assumed as rational and the players believe that their opponents act rationally throughout the game. Based on which the common utility function is maximized to derive the optimal strategy. However, the underlying rationality assumption is often unrealistic. This situation is avoided in evolutionary games by introducing the concept of bounded rationality, where players adopt dynamic strategies that lead them to sustain in the population without caring about instant payoff maximization. This dynamic strategy alteration process eventually leads the individuals to achieve the equilibrium solution.
3. **Game Dynamics**: Since players in the evolutionary games interact with each other in the population for multiple rounds by adopting different strategies, the state of the interaction game varies over time according to the replicator dynamics. Thus, the evolutionary game provides a natural way to introduce dynamics in the system, where successful strategies are imitated by other individuals and propagate over interaction rounds. In particular, the state of the evolutionary game at any point can be captured using the replicator dynamics, which becomes very handy to understand the evolution trajectory of players’ behaviors/strategies over time.

### 3.3 Analyzing CYBEX Participation Game

Once the problems are identified and the game is formalized, we need to solve the game for the firms. Solving a game means predicting the steady state strategy of each rational player given the information observed from the game. Hence, we aim to find the equilibrium strategy of each player that is mutually best response with respect to other players’ actions. Most importantly, it is necessary to know if such equilibrium strategy exists, whether it is evolutionarily stable or not, i.e. no small group of players adopting different strategy could invade the rest of population.

In this section, we now analyze the CYBEX participation game in-depth and investigate if the game has ESS and under what conditions. We are particularly interested in modeling cyberinsurance which can be used as an initial incentive to attract the firms to share in the CYBEX framework. The system is aimed to be independent and self-enforced, so that the information sharing nature of
Chapter 3. **Self-Coexistence of Firms in CYBEX Framework**

the firms is enhanced even without any external stimulant, which will help the system to reach ESS in a self-enforced manner.

As far as a decision strategy in this game model is concerned, every firm has the binary strategy set:

\[ S = \{ \text{Participate and Share in CYBEX, Not Participate} \} \] (3.1)

With the strategy set defined, we now define the pairwise strategic form payoffs in Table 3.1, when any two of the firms engage in pairwise interaction.

<table>
<thead>
<tr>
<th>Payoffs in Strategic–Form for Participation Game</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participate &amp; Share</td>
</tr>
<tr>
<td>( Sa \log(1 + I) - x - c, )</td>
</tr>
<tr>
<td>( a \log(1 + I), )</td>
</tr>
<tr>
<td>( a \log(1 + I) - x - c )</td>
</tr>
</tbody>
</table>

When firms are not involved in the CYBEX framework (i.e., they neither participate nor share), the utility reward to the firms is dependent on only their own investment, which can be presented as the following variant of logarithmic function, \( a \log(1 + I) \), where \( I \) is the amount of investment made by the firms and \( a \) is a simple scaling parameter that maps user satisfaction/benefit to a dimension equitable to the price/monitory value [92][93]. For the rationality constraint, \( a \log(1 + I) > 0 \) must be held, otherwise, the firms would prefer to not make any investment. The logarithmic gain function motivates the players by rewarding for increasing steps towards security investment. However, the reward eventually saturates with gradually increasing investment. This is because increasing the investment further even beyond a certain threshold does not necessarily increase the overall utility with a high rate of increment, rather
limiting and saturating the reward obtained [92][93]. In this symmetric game work, we assumed a fixed information sharing by every participant, which is also considered as maximum available information to a firm. To analyze the sharing scenario more realistically, we later extend this work to formulate an information sharing game, where firms have choices to share different amount of cybersecurity information.

We also assume, when the engaged firms participate in mutual sharing, the resulting benefit for them would then stem, not just from their own investment, but also from their sharing. Thus we consider this utility (when both the firms sharing mutually) as $S_a \log(1 + I)$, which can be considered as return on both investment and sharing. Again for the rationality constraint, $S > 1$, otherwise the player does not have any incentive of sharing. $c$ is the cost of participation in the CYBEX architecture, i.e., the amount charged by CYBEX system of governance for participating and $x$ reflects the cost of information sharing as explained earlier in Subsection 3.1.3.

However, when a pair of firms are mutually interacting, while one of them is part of CYBEX and the other is not, then the utility to the firms are given in the top right corner and bottom left corner cells. This scenario depicts the risk of participating, where the participating firm incurs the cost due to participation in CYBEX without any additional sharing gain and the other non-participating firm incurring no cost but also not gaining anything due to not sharing. Note that, we could always use any other complex values or functions for depicting the utilities and cost, however, our aim here is to analyze the ESS and its conditions in the game regardless of the exact utility or cost values as long as the nature of utility and the costs follow the rationality constraints as required in a real
market. For the ESS analysis, we model this game as a symmetric game and derive various conditions under which different ESSs can be achieved.

**ESS Analysis of this game:**

To analyze the evolutionary stability of the game, we assume $\alpha \in [0, 1]$ is the proportion of population participating and sharing in CYBEX. Then, according to replicator dynamics [89, 94], the transformation speed can be given by

$$g(\alpha) = \alpha \left[ E_{sh}(u) - E(u) \right]$$

(3.2)

where, $E_{sh}(u)$ is the expected payoff of a player for participating and sharing, and $E(u)$ is the average payoff in the population. The expected utility of “participate & share” strategy can be given as

$$E_{sh}(u) = \alpha \left[ Sa \log(1 + I) - x - c \right] + (1 - \alpha) \left[ a \log(1 + I) - x - c \right]$$

(3.3)

Similarly, $E_{not}(u)$ is the expected payoff of a player for not sharing, where $E_{not}(u) = a \log(1 + I)$. Hence,

$$E(u) = \alpha \left[ E_{sh}(u) \right] + (1 - \alpha) \left[ E_{not}(u) \right]$$

The replicator equation given in Eqn. (3.2) can be rewritten as:

$$g(\alpha) = \alpha \left[ \alpha (Sa \log(1 + I) - x - c) + (1 - \alpha) (a \log(1 + I) - x - c) \right.$$

$$- \alpha E_{sh}(u) - (1 - \alpha) a \log(1 + I)]$$

(3.4)
After simplifications,

\[ g(\alpha) = \alpha(1 - \alpha) [\alpha(S - 1)a \log(1 + I) - x - c] \]  

(3.5)

For ESS to be achieved, there are two conditions [89, 94]: (1) the transformation rate should be zero, i.e., \( g(\alpha) = 0 \), and (2) the neighborhood of the equilibrium states (found through condition (1)) must also be stable. To prove a strategy to be evolutionarily stable, it is necessary to verify that the population playing with ESS cannot be invaded by any other individual(s) playing with strategy other than ESS. If condition (2) is not met, then there is a chance that any small subgroup of player playing with a random strategy other than ESS can invade the total population of players playing ESS.

For the transformation rate to be zero, i.e., \( g(\alpha) = 0 \), there exists three distinct solutions of \( \alpha \), (i.e., three potential equilibrium states):

\[ \alpha_{sol_1} = 0 \]  

(3.6)

\[ \alpha_{sol_2} = 1 \]  

(3.7)

\[ \alpha_{sol_3} = \frac{x + c}{(S - 1)a \log(1 + I)} \]  

(3.8)

With these three potential equilibrium states, we now need to check the stability of their neighborhood and then only the equilibrium states can be recognized as ESS. For the neighborhood strategies to be stable, the condition of \( g'(\alpha) < 0 \) must hold true at each of the equilibrium states. With the three solutions of \( \alpha \), it is found that

\[ g'(\alpha_{sol_1}^*) = 0 = -x - c \]  

(3.9)
Therefore it is clear that ESS is conditioned upon the wise choice of incentives and participation costs (cyberinsurance $c$) and that cyberinsurance can be used to motivate the socially optimal behavior and deter non-cooperative behaviors. Next, we analyze each of the conditional constraints for ESS and show under what bounds the population will evolve toward sharing and under what bounds they would not.

### 3.3.1 Analyzing conditional constraints for ESS

As can be seen in the following, we analyze all possible conditional constraints for ESS, depending on the cyberinsurance $c$, governed by the CYBEX system for governance. Note that, the cost of information exchange, $x > 0$ as this is an inherent cost by the firms for information sharing.

**Case (i):** Let us first assume, $c > 0$ & $c \geq (S - 1)a \log(1 + I)$. Therefore, $g'(\alpha_{sol_1}^* = 0) < 0$ and $g'(\alpha_{sol_2}^* = 1) > 0$.

It can be seen that $g'(\alpha_{sol_3}^*)$ itself does not hold as $\alpha_{sol_3}^* > 1$. However, it must lie between 0 and 1. Hence $\alpha_{sol_1}^* = 0$ is the only ESS under this condition, which implies that evolutionary stable strategy for the population would be to “not participate” in the CYBEX architecture due to high cost for such activity. Though it is intuitive that the population will never participate in the sharing framework because of high participation cost ($c$), this cost has an important role in motivating the players to participate, which is discussed in the later case. For

\[
g'(\alpha_{sol_2}^* = 1) = -(S - 1)a \log(1 + I) + x + c \quad (3.10)
\]

\[
g'(\alpha_{sol_3}^*) = \frac{x + c}{(S - 1)a \log(1 + I)} \quad (3.11)
\]
numerical analysis, we show a simple scenario following the above conditions even when the evolutionary game initiates from a high “participate & share” population proportion $\alpha^* = 0.8$, it is found from Fig. 3.1 that the individuals taking “Not Participate” strategy could successfully invade the individuals that are participating and sharing because of no cost for taking “Not Participate” strategy. For all the results found from numerical analysis, we assumed the rationality constant $S = 2$; scaling constant $a = 3$; and investment $(I)$ as 5 units. The values of participation cost $(c)$ and cost of information sharing $(x)$ are suitably varied for different cases based on each condition. For this case, we assumed $c = 7.4$, and $x = 3$ units.

![Figure 3.1: Population proportion variation under constraint (i)](image)

**Case (ii):** When $c > 0 \& c < (S-1)a \log(1+I)$ such that $(c+x) \geq (S-1)a \log(1+I)$. Therefore, $g'(\alpha_{sol1}^* = 0) < 0$ and $g'(\alpha_{sol2}^* = 1) > 0$

It can be seen that $g'(\alpha_{sol3}^*)$ itself does not hold true, as $\alpha_{sol3}^*$ does not lie between 0 and 1. Hence, under this condition, again, $\alpha_{sol1}^* = 0$ is the only ESS implying that evolutionary stable strategy for the population would still be not to participate in the CYBEX architecture regardless of the initial participating strategy population. As the total cost component exceeds the sharing gain in this case, the initial...
population taking the “Participate and Share” strategy can easily be invaded by a small group of individuals taking the “Not Participate” strategy. The result from numerical analysis is presented in Fig. 3.2 by assuming \( c = 3.4 \) and \( x = 3 \), which demonstrates that irrespective of any initial \( \alpha \) value, the ESS is always found to be “Not Participate” strategy and always gets invaded by the population of “Participate and Share” strategy.

**Figure 3.2:** Population proportion variation under constraint (ii)

**Case (iii):** When \( c > 0 \) & \( c < (S-1)a \log(1+I) \) such that \( (c+x) < (S-1)a \log(1+I) \). Therefore,

\[
\begin{align*}
g'(\alpha_{sol1}^*) &= 0 < 0 \\
g'(\alpha_{sol2}^*) &= 1 \times 0 \\
g'((\alpha_{sol3}^*) &= (c+x)\left[1 - \frac{c+x}{(S-1)a \log(1+I)}\right] \\
g'((\alpha_{sol3}^*) &= 0
\end{align*}
\]

Hence, two possible ESS (\( \alpha_{sol1}^* = 0 \) and \( \alpha_{sol2}^* = 1 \)) exist in this case, however, achieving a particular ESS depends on the initial “participate and share” population distribution. ESS tends to “Not Participate” if \( 0 < \alpha^* < \frac{c+x}{(S-1)a \log(1+I)} \) and ESS tends to “Participate and Share” if \( \frac{c+x}{(S-1)a \log(1+I)} < \alpha^* < 1 \), where \( \alpha^* \) is...
the initial population fraction playing with participate and share strategy. This clearly implies that if the initial “Participate & Share” population fraction is more than a certain threshold/tipping value, \( \alpha_{\text{thres}} = \frac{c+x}{(5-1)\alpha \log(1+t)} \), then the rest of the population fraction (which are not sharing) will evolve over time and will participate in CYBEX, thus ESS tends toward “Participate and Share” strategy. Alternatively, if the initial “Participate & Share” population fraction is less than \( \alpha_{\text{thres}} \), then the gain from the system would not be sufficient enough to enforce the entire population toward full participation. However, ESS will tend towards “Not Participate” strategy, thus showing the significance of the initial “Participate and Share” population strength as well as the significance of cyberinsurance/participation cost \( c \). Fig. 3.3 presents two sample numerical results where the initial population proportion of “Participate and Share” strategy \( \alpha^* = 0.65 \) and 0.9 respectively, assuming \( c = 2.4, x = 1.5 \). The simulation results validate the deflecting nature of ESS based on the theoretical threshold/tipping value that can be computed numerically by using the \( \alpha_{\text{thres}} \) expression, and found to be 0.72. From Fig. 3.3(a), it is shown that most individuals lean towards the “Not Participate” strategy, when the initial participating population proportion \( \alpha^* \) is below the threshold value. However, when the initial “Participate and Share” population is above the threshold value, the population evolves towards more participation as shown in Fig. 3.3(b). The expected individual utility is the reason for this kind of deflection in ESS because the average utility to a firm playing “Not Participate” strategy is more, when less players are playing the same strategy, compared to the “Participate and Share” strategy and vice-versa.

**Case (iv):** When \( c < 0 \) such that \( (c + x) \leq 0 \), i.e., the cost of participation is negative implying the fact that it is no longer a cost but rather a positive
incentive given to the firms for enrolling in CYBEX architecture. Therefore, 
\[ g'(\alpha^*_\text{sol}_1 = 0) > 0 \] and 
\[ g'(\alpha^*_\text{sol}_2 = 1) < 0 \]

It is clear that \( g'(\alpha^*_\text{sol}_3) \) itself does not hold true. Hence \( \alpha^*_\text{sol}_1 = 0 \) is the only ESS under this condition, which implies that ESS for the population would be to participate and share in the CYBEX architecture regardless of initial \( \alpha^* \) value. According to this case, the total cost \((c + x)\), appears to be an incentive for firms to participate, hence the population will eventually be inclined towards the “Participate & Share” strategy irrespective of any \( \alpha^* \) value as shown in Fig. 3.4, where \( c + x \) is assumed to be -1. The result shows that the individuals with “Participate and Share” strategy could successfully invade the “Not Participate” strategy individuals.

**Figure 3.3:** Population proportion variation under constraint (iii)

**Figure 3.4:** Population proportion variation under constraint (iv)
Remark: Hence, ESS is not unique for the CYBEX participation game. Both strategies “Participate & Share” and “No Participate” have potential to be evolutionarily stable depending on which of the above presented cases are satisfied.

To give a clear picture that the CYBEX participation game has two potential evolutionary equilibrium strategies that are dependent on certain conditions as given above, Fig. 3.5 encapsulates the summary of above discussions. We can see that when the case (i) or (ii) is satisfied, the population preferably chooses “No Participate” strategy to be evolutionarily stable, whereas Participate strategy happens to be the ESS, when case (iv) is satisfied. The most interesting scenario of our model is the condition (iii), where both “Participate” and “No Participate” strategy could possibly be ESS but dependent on the initial proportion of participants in CYBEX. These ESSs can be triggered based on the appropriate incentive/cost from CYBEX.
3.3.2 Understanding the impact of conditional constraints on firms’ participation

Guidance for CYBEX: The above discussion illustrates how the evolutionary stability structure of CYBEX is directly dependent on the incentive/participation cost along with initial “Participating” population strategies. Thus, it is of utmost importance to model the cost of participation according to the conditional constraints presented in above model to establish and maintain an effective CYBEX system. These conditions not only show that ESS can be achieved, but also demonstrate how the participation cost is a factor for improving participation in CYBEX and the utility obtained through sharing.

Since CYBEX is also a rational player in the participation game, its aim is to charge a cost to the firms for their participation. To do so, if CYBEX introduces a flat participation cost, then it is possible that firms will not be interested to take part in the framework as positive cost may dominate over sharing gain. Hence, the goal of CYBEX, i.e. cyber-threat information sharing, may not be fulfilled. However, if CYBEX provides incentives for firms’ participation, then CYBEX cannot gain anything in return as it goes against its rationality. Hence, a dynamic cost of participation mechanism is necessary to let both CYBEX and firms coexist in a sharing market such that firms can take the advantage of information sharing and CYBEX can profitably manage the participation as well as CTI sharing, thus leading us to present Algorithm 1.

Our proposed algorithm works in the following manner. At the start of the game, when the initial strength of participating population is very small in CYBEX, our analysis shows that using case (iv), incentives can be given to help
and evolve the system toward more participation rather than charging with a cost for participation. Once the system goes beyond the threshold (in terms of number of players enrolled in CYBEX), then moving into case (iii), would still ensure that the system will self-sustain in terms of participation without any external positive incentive. Now CYBEX can impose a particular cost for participation knowing how many participants are in the system. The same process is repeated to impose the set of participation costs iteratively. Thus, the dynamic cost adaptation algorithm can provision benefits to CYBEX by maximizing the participation in the system, thus providing benefits to both the participants and CYBEX.

It should be noted that the algorithm does not require lot of information and exchange prior to making decisions. However, in our algorithm a small set of parameters are required to be exchanged with CYBEX for only once, which are the fixed values for each firm. Since our algorithm considers that all the firms are homogeneous in nature, the parameters remain same across all other players too. The necessary information that need to be exchanged with CYBEX are the sharing cost \( x \), investment \( I \) amount of a firm, and rationality constant for sharing \( S \). CYBEX can use all these parameters to calculate what proportion of participants in the system is needed to impose a particular participation cost. Therefore, these information are not required to be exchanged multiple times with CYBEX but only once. As the game progresses, CYBEX counts the number of enrollments and uses it to know which cost \( c \) from the set of all participation costs it can charge to the firms.

In the algorithm 1, the set of \( k \) ordered participation costs are stored in the array \( CYBEX\_Cost\_INC[1 \cdots k] \). In line 2, we initialize the incentive \( c \) from
CYBEX. The initial proportion of participants ($\alpha$) is assumed to be very small (say $\epsilon$). At stage $t = 0$, the individuals initialize their probability of choosing “Participate” strategy ($p^i(0)$) to $\epsilon$ and probability of choosing “Not Participate” to $1 - \epsilon$. At stage $t = 1$, CYBEX plans to enforce a minimum participation cost ($c$) of $CYBEX.Cost.INC[1]$, but to do that it has to wait until proportion of participating population reaches to at least $\alpha_{thres} = \frac{CYBEX.Cost.INC[1]+x}{(S-1)\alpha \log(1+x)} \times |N|$. After this goal is achieved, the players participating in CYBEX need to pay $c = CYBEX.Cost.INC[1]$ amount. In line 12-21, each player takes its action based on its mixed strategy probability vector and CYBEX imposes a participation cost if number of participants exceeds the threshold. Based on the cost, the players calculate an updated payoff which is also used to update their mixed strategy probability vector. This process is repeated for all players until each of the $k$ participation costs is successfully charged or maximum number of game stages is reached.

### 3.3.3 Learning heuristic for evolutionary stable strategy

In the previous section, we presented the detailed theoretical analysis and impact of conditional constraints for ESS, which clearly demonstrates how CYBEX architecture can dynamically induce cyberinsurance (participation) cost/incentive to attract and self-enforce firms toward sharing and achieve stability. However, in a simultaneous distributed non-cooperative CYBEX participation game, it is also necessary to design a distributed learning heuristic for the firms to decide which strategy to play at each stage, and how to update their “strategy selection probability” based on the utility feedback obtained from the past game stages.
Algorithm 1: Dynamic Cost Adaptation algorithm

1 **Assumptions:** CYBEX has \( k \) of different costs to ask the firms.
2 **Data:** \( S, I, x, \kappa \) and \( CYBEX\_Cost\_INC[1...k] \)
3 **Result:** Participant population proportion (\( \alpha \)) to reach 100%

4 Initialize \( c \) with a value s.t. \( c < 0 \) and \( c + x < 0 \);
5 \( \alpha \leftarrow \epsilon \), where \( 0 < \epsilon << 1 \);
6 Payoff\_matrix \leftarrow \text{calculate\_payoff}(c);
7 \( k_1 \leftarrow 1 \);
8 **for** \( t \leftarrow 1 \) to \( \text{max}T \) **do**
9 \( \alpha_{\text{thres}} \leftarrow \frac{CYBEX\_Cost\_INC[k_i] + x}{(S-1)\ln \log(1+I)} \);
10 **for each** \( i \in N \), **do**
11 \( \text{Take a uniform random strategy decision based on} \)
12 \( p^i = [p^i_1(t-1), p^i_2(t-1)]; \)
13 \( \alpha_{\text{new}} \leftarrow \frac{1}{|N|} \times \text{count\_participants}(); \)
14 \( \text{if} \alpha_{\text{new}} > \alpha_{\text{thres}} \text{ and } k_i \leq k \text{ then} \)
15 \( c \leftarrow CYBEX\_Cost\_INC[k_i]; \)
16 \( k_i \leftarrow k_i + 1; \)
17 \( \text{Payoff\_matrix} \leftarrow \text{calculate\_payoff}(c); \)
18 **end**
19 \( U_i(t) \leftarrow \text{Pairwise\_Interaction(Payoff\_matrix)}; \)
20 **Update the strategy selection probability** \( p^i_1 \) **according to**
21 \( p^i_1(t) = p^i_1(t-1) + \kappa(U_i(t) - U_{i,1}^\text{avg}(t)) \)
22 \( p^i_2(t) = 1 - p^i_1(t) \)
23 \( \text{// } U_{i,1}^\text{avg}(t) : \text{Avg. payoff from “Participate” strategy until stage } t \)
24 **end**

As the game unfolds, the firms would then learn about their best responses and eventually converge to ESS.

In the following, we detail the description of the distributed learning algorithm for the firms to obtain ESS by following the natural evolution similar to replicator dynamics. For choosing a strategy based on the firms' past experience, each firm \( i \in N \), maintains a probability vector, \( p^{(i)}(t) = \{(p^{(i)}_1(t), p^{(i)}_2(t)) : p^{(i)}_1(t) + p^{(i)}_2(t) = 1\} \)
Chapter 3. Self-Coexistence of Firms in CYBEX Framework

1}, which defines the probability of choosing “Participate & Share” and “Not Participate” strategy by firm $i$ at game stage $t$ respectively. In each stage, all possible pairwise simultaneous interactions are conducted from each firm’s perspective, where, each firm $i \in N$ sticks to a single strategy throughout the stage and observes the average pairwise utility $\bar{U}_{pair}^{(i)}(t)$ for stage $t$.

$$
\bar{U}_{pair}^{(i)}(t) = \frac{\sum_{j \neq i} U_i^{(t)}(s_i, s_j)}{|N| - 1}
$$

where, $U_i^{(t)}(s_i, s_j)$ is the payoff to player $i$ from the simultaneous pairwise game between firm $i$ and $j$ by playing with strategy $s_i$ and $s_j$ respectively at game stage $t$.

After each game stage, the player $i$ update its probability of selecting strategy $s_i$ by utilizing two different average utility vectors: (1) $\bar{U}_{avg}^{(i)}(t)$: average received utility, and (2) $\bar{U}_{s_i \in S}^{(i)}(t)$: average utility obtained by playing “strategy $s_i$ only” until stage $t$, which are defined as follows:

$$
\bar{U}_{avg}^{(i)}(T) = \frac{\sum_{t=1}^{T} \bar{U}_{pair}^{(i)}(t)}{T}
$$

$$
\bar{U}_{s_i \in S}^{(i)}(T) = \frac{\sum_{t=0}^{T} \{ \bar{U}_{pair}^{(i)}(t) | a_i(t) = s_i \}}{T'}
$$

where, $a_i(t)$ is the action of player $i$ at game stage $t$ and player $i$ played strategy $s_i$ for $T'$ number of stages until stage $T$, such that $T' \leq T$.

To learn a stable strategy from the strategy set $S$, the probability of choosing a particular strategy must be reflected from the average utility it receives by playing that strategy. Hence the difference between player $i$’s average utility obtained by playing a particular strategy $s_i$ and average utility out of all game
stages will help to decide the probability of choosing $s_i$ in future. Assuming player $i$ played strategy $s_i \in S$ at $(t - 1)^{th}$ stage, the probability of playing the same strategy ($p_{s_i}^{(i)}(t)$) at $t^{th}$ stage can be computed using the update rule given in Eqn. (3.16) and the probability of playing with complementary strategy ($s'_i$) can be given as: $p_{s'_i}^{(i)}(t) = 1 - p_{s_i}^{(i)}(t)$.

Algorithm 2: Learning Heuristic for ESS Convergence

1. Initialize the initial “participating” population proportion $\alpha(0)$ for “Participate and Share” strategy, and utility matrix $U$;
2. Initialize random strategy profile, $p^{(i)}(0) = (p_1^{(i)}(0), 1 - p_1^{(i)}(0)) \forall i \in \mathcal{N}$;
3. while $\text{stage } t \leq \text{Max}T$ do
   4. for each firm $i \in \mathcal{N}$ do
      5. Select a strategy $s_i \in S$ based on its mixed strategy profile $p^{(i)}(t)$;
      6. Observe the average utility reward $\bar{U}_i^{(i)}(t)$ from all simultaneous pairwise interactions;
      7. Update the probability of selecting strategy $s_i$ ($p_{s_i}^{(i)}(t + 1)$) for player $i$ according to equation 3.16;
      8. Update the probability of playing with complementary strategy $s'_i$ as ($1 - p_{s_i}^{(i)}(t + 1)$);
   9. $t \leftarrow t + 1$;
10. end
11. end

where, $\kappa \in (0, 1)$ represents the learning constant that determines how fast or slow the players will move towards the optimal probability of choosing a particular strategy. It is an input parameter for the learning algorithm and must be chosen wisely for faster convergence. If $\kappa$ is too small, then they require more iterations to converge, however, if $\kappa$ is very large, the players might skip the optimal solution. The game is played repeatedly until the probability of choosing certain action becomes stable and does not change more than a small value $\epsilon > 0$ over the stages. The Algorithm 11 summarizes the distributed learning heuristic.
which is employed by the players to learn and play with ESS eventually.

\[ p_{s_i}(t) = p_{s_i}(t-1) + \kappa (\bar{U}_{s_i}(t) - \bar{U}_{avg}(t)) \] (3.15)

The following lemma helps to prove the convergence of the proposed learning heuristic to an ESS.

**Lemma 3.1.** The sequence of processes \( \{P(t)\} \), where \( P(t) = (P_1(t), P_2(t), \ldots, P_N(t)) \) be the state of the population at stage \( t \), converges as the learning constant \( \kappa \to 0 \).

**Proof:** Without loss of generality, a player \( i \) in the game updates its probability of choosing a strategy \( s_i \) using the following update rule.

\[ p_{s_i}(t) = p_{s_i}(t-1) + \kappa (\bar{U}_{s_i}(t) - \bar{U}_{avg}(t)) \] (3.16)

where, \( \bar{U}_{avg}(T) = \frac{\sum_{t=1}^{T} \bar{U}_{pair}(t)}{T} \) (3.17)

\[ \bar{U}_{s_i \in S}(T) = \frac{\sum_{t=0}^{T} \{ \bar{U}_{pair}(t) | a_i(t) = s_i \}}{T'} \] (3.18)

We consider that \( \bar{U}_{pair}(t) \) is the average utility observed by the player \( i \) at stage \( t \) for all possible pairwise interactions in the population.

Now we can consider that \( P(t) = (P_1(t), P_2(t), \ldots, P_N(t)) \) be the state of the population at stage \( t \), where \( P_i(t) = \{ p_{s_i}^{(i)}(t), p_{s_i'}^{(i)}(t) \} \) such that \( p_{s_i}^{(i)}(t) + p_{s_i'}^{(i)}(t) = 1 \). From the learning rule given in Eqn. 3.16, we can see that probability of choosing a strategy is dependent on the previous stage probability and the accumulated utility until current stage. Hence it is clear that \( \{P(t) : t \geq 0\} \) is a Markov process. To prove that the learning process eventually converges to an equilibrium strategy, we basically need to analyze the asymptotic behavior.
of \{P(t)\} when the learning constant \(\kappa \to 0\). We can apply the Theorem 3.2 from [95] (presented below) and state that when \(\kappa \to 0\), the Markovian sequence \{P(t)\} converges to the solution of following ordinary differential equation.

\[
\frac{dP}{dt} = f(P), \; P(0) = f(0) \quad (3.19)
\]

where, \(P(0)\) is the initial strategy selection probability of the population and \(f(P)\) is the conditional expected function defined as:

\[
f(P) = \mathbb{E}[G(P(t), \tilde{U}^{(i)}_{s_i \in S}(T), \tilde{U}_{avg}(T), a(t))|P(t)] \quad (3.20)
\]

where, \(G(\cdots)\) can be correlated with Eqn.3.16 by considering the learning equation for the population as \(P(t) = P(t - 1) + \kappa G(P(t), \tilde{U}^{(i)}_{s_i \in S}(T), \tilde{U}_{avg}(T), a_i(t))\).

**Theorem 3.2.** Consider the sequence of interpolated processes \(\{P_b(.)\}\). Let \(X_0 = P_b(0) = P(0)\). Then the sequence converges weakly, as \(b \to 0\) to \(X(.)\) which is a solution of the ODE, \(\frac{dX}{dt} = f(X), X(0) = X_0\) [95].

The above theorem is a particular case of generalized result presented in Theorem 3.2 of Kushner [96], which can be stated as follows.

**Theorem 3.3.** Assuming the conditions of Canonical algorithm [96], each subsequence of \(\{\theta^\epsilon(q_\epsilon + \cdot), \epsilon > 0\}\) has a further subsequence which converges weakly to a bounded solution \(\theta(.)\) of \(\dot{\theta} = g(\theta)\) on \([0, \infty)\) if \(q_\epsilon = 0\) and on \((-\infty, \infty)\) if \(q_\epsilon \epsilon \to \infty\), where \(g(.)\) is a continuous function of \(\theta\) [96].
Chapter 3. **Self-Coexistence of Firms in CYBEX Framework**

Using the above theorem, we can note the following points about our learning algorithm.

1. It is true that \( \{P(t), (a(t-1), U_{\text{diff}}(t-1)), t > 0 \} \) is a Markov process, where 
   \[ U_{\text{diff}}(t) = \bar{U}_{s_i}(t) - \bar{U}_{\text{avg}}(t) \]. Additionally, the tuple \((a(t), U_{\text{diff}}(t))\) takes value from the compact metric space.

2. The function \( G(\cdots) \) is a continuous and bounded function.

3. If \( P(t) = P \) is a constant at stage \( t \), then the process \( \{(a(t), U_{\text{diff}}(t), t > 0) \} \) is i.i.d. sequence.

4. The differential equation given in Eq. 3.19 has a unique solution for every initial condition.

Using Theorem 3.3 from [96], it can be stated that the sequence \( \{P(t)\} \) converges to the solution of the differential equation presented in Eqn. 3.19 when the learning constant \( \kappa \to 0 \). Hence the lemma follows.

It is evident that the individuals preferably take an action that could lead them to survive in the population. According to the learning rule provided in Eqn. 3.16, we can state that if the pairwise interactions provide higher utility for taking a certain strategy then the individuals can invade the rest of the unsuccessful strategies in the population, hence leading to a stable equilibrium strategy. As in our model, we have two pure strategies available for the players, and both can potentially be evolutionarily stable, our algorithm always leads to one of the pure strategy solutions.
3.3.4 Results and Discussion

In this subsection, we present the simulation results that have been obtained from the proposed distributed learning heuristic to attain ESS under different conditions. The population size is assumed as 100 for all the simulation scenarios. The rationality constant \( a \) and investment \( I \) are assumed to be 2, and 5 units respectively, which are kept same for all the experiments. The value of sharing cost \( (x) \) and participation cost \( (c) \) is varied dynamically to maintain different conditions described in Section 6.2. The learning constant \( (\kappa) \) is assumed to be 0.07. Each stage represents all the possible simultaneous pairwise interactions between the players, and they play 500 such stages in each experiment. Unless otherwise mentioned, the initial “Participate and Share” strategy population proportion is considered as 65%.

![Graph (a) Average utility growth](image1.png)

![Graph (b) Evolution of “Participate and Share” strategy population under different participation cost](image2.png)

**FIGURE 3.6:** (a) Average utility growth, (b) Evolution of “Participate and Share” strategy population under different participation cost

In Fig. 3.6(a), we plot the evolution of average utility over the number of stages for different cost \( (c) \) values. It is observed that when the cost of participation \( (c) \)
is negative, the individuals find an incentive to participate and share. However, when $c > 0$, the individuals choose to take part and share in the framework opportunistically depending on how many other players participate and share in the framework. Therefore, the average utility converges at high value when the participation cost is minimum, where the population unanimously play the “Participate & Share” strategy. As $c$ increases above certain threshold, the individuals find that participating in sharing is costly and switch to “Not Participate” strategy, which is why the saturated average utility is less for $c = 4$ than $1$. It is shown that the proposed heuristic helps the individuals reach the evolutionary stable state within fewer game stages by making them learn about the expected utilities of different strategies. We experimented to understand how quickly the population adapts to ESS, we plot the growth of “Participate and Share” strategy population in Fig. 3.6(b). It is clear that a population type either invades another type or gets invaded by the other type depending on the cost constraints. If the participation cost ($c$) is negative, then it is intuitive that everybody will be willingly participate and share because the participation cost is nothing but an incentive. However, when the cost is positive, then the stable strategy depends on how many other members adopt that particular strategy. In our experimental setup, the population converge to “Participate and Share” when the initial sharing strategy population is 65% or more and cost ($c$) is 1, but they get invaded by the rest of “Not Participate” strategy individuals if $c$ increases to 4 because the tipping point requirement is now well above 65%. The important point to notice here is the convergence speed of the proposed learning heuristic, which enables the firms to obtain their ESSs within very few number of game stages.

In Fig. 3.7, we present the evolution of average utility with respect to different values of learning rate $\kappa$. The reason of having this experiment is to understand
which learning rate would preferably help the system to quickly reach ESS. It is found that low as well as high $\kappa$ value take relatively longer time to stabilize the average utility because low $\kappa$ takes longer duration to reach the optimal selection probability and high $\kappa$ oscillates around the optimal solution. Hence, the step size $\kappa$ must be chosen carefully to achieve quick convergence to the equilibrium strategy. From the result reported, we observed that the value of $\kappa$ in the range of 0.05 to 0.09 works better for our simulation and helps the players to quickly adapt to the evolutionary strategy. To understand how our proposed dynamic participation cost/incentive can help CYBEX to increase its revenue, we simulate two scenarios presented in Fig. 3.8: where (1) 95% individuals initiated with “participate and sharing” strategy in the beginning but CYBEX charges a static amount ($c = 5$) towards participation all along, and (2) CYBEX uses our proposed dynamic participation cost/incentive mechanism (based on
conditions of case (iii & iv) presented in Section 6.2), even when only 5% of total population were sharing at starting. It is observed that in the scenario (1), the participating population percentage decreases over stages due to the high cost charged by CYBEX (as seen in Fig. 3.8, in red color plot). It is also seen that the cumulative revenue of CYBEX over time does not increase any more as firms leave the framework gradually (as seen in Fig. 3.9, in red color plot). However in scenario (2), CYBEX could manage to attract more firms to participate by rewarding \((-c = 0.5)\) them in the beginning. As the number of participants started growing (going beyond the population threshold/tipping point as given in case (iii), Section 6.2), CYBEX dynamically updates its participation cost within a certain limit (based on the cost conditions presented in case (iii), Section 6.2) to generate revenue. But it ensures that the cost raise do not lead the participating population to leave the framework rather it can still attract more participants to join so that eventually every firm will be inside the sharing framework. Thus
CYBEX’s incremental cost raise can lead to a win-win situation, where every firm participates and shares to strengthen their security infrastructure, and CYBEX also generates an increasing revenue as depicted in Fig. 3.8, and 3.9 respectively (blue color plots).

In our next set of simulation results presented in Fig. 3.10 and Fig. 3.11, we demonstrate the evolution of the population, when cost of participation \( (c) \) is varied and initial participant population is below/above than 50%. At a participation cost of 1, it is observed that case (3) gets satisfied until \( x \) reaches 3.5. But we know that as \( x \) increases, the value of required participation threshold \( (\alpha_{thres}) \) increases too. We can find that, for \( x = 0.5, 1.5, 2.5, 3.5 \), the required \( \alpha_{thres} = 0.28, 0.47, 0.651, 0.84 \) respectively. Hence, the population can converge to “Participate” strategy when \( x = 0.5 \) and 1.5, provided \( \alpha_{init} = 0.65 \), which is true according to Fig3.10a. But, when \( \alpha_{init} = 0.4 \), the population can converge to “Participate” strategy when \( x = 0.5 \) only as seen in Fig. 3.11b. However, when
sharing cost \((x)\) increases beyond 3.5, the total cost dominates over the sharing gain and hence case (1) or (2) is triggered, which is why “No Participate” strategy turns out to be evolutionarily stable.

If the participation cost is raised to 2, and cost of sharing is high \((x > 1.5)\), then the cost component exceeds over the total gain, hence case (1) or (2) becomes applicable. We can see in Fig. 3.10b and Fig. 3.11c that high \(x\) always disappoints the population, leading to zero participation eventually. Since the low value of \(x\) can enforce the case (3), it requires at least 27% and 47% participants for \(x = 0.5\) and 1.5 respectively, which cannot be satisfied when \(\alpha_{init} = 0.4\) as shown in Fig. 3.11c. However, the population can converge to full participation in case of \(\alpha_{init} = 0.65\) as shown in Fig. 3.10b. When the participation cost increases to 3 or more, then high sharing cost will always lead to no participation in the framework as we have seen in above cases. Fig. 3.10c verifies that when \(x\) is high, the case (1) or (2) is induced that leads the system to no participation altogether. When sharing cost is small, the strength of participating population is not enough to enforce all firms toward participation. However, when cost of participation is negative, i.e. CYBEX is providing incentives for participation, then firms would prefer to participate if the sharing cost is not dominating over the sharing benefits. We can observe from Fig. 3.11a that when \(c = -2\) and \(x < 2\), the firms always get profit out of participation, hence it is wise for each firm to participate. However, as the cost of sharing increases gradually, firms’ behavior changes because of higher cost, which is why the evolutionary stable strategy for the population turns out to be “No Participate”.

**Remarks:** Since research in the CYBEX domain is still in its inception, there does not exist any standardized sharing platform yet to provide us actual field-data.
Chapter 3. *Self-Coexistence of Firms in CYBEX Framework* 79

**Figure 3.10**: Evolution of participating population at different participation cost, when initial participant proportion is 0.65

(A) Cost of participation ($c = 1$)

(B) Cost of participation ($c = 2$)

(C) Cost of participation ($c = 3$)
Figure 3.11: Evolution of participating population at different sharing cost, when initial participant proportion is 0.4
Chapter 3. Self-Coexistence of Firms in CYBEX Framework

Due to the lack of such field-data, our selection for parameter values not only adheres to the real-world rationality constraints but also conveys how these values would originate in the real-world. The values of the participation cost in Fig. 3.10 are 1, 2, and 3. While one can quibble that maximum costs may not be shown, as opposed to appropriate costs, these value assignments lay the stage for a conventional participant’s expectations. First, a compulsory up-front unit cost (i.e., $c = 1$) is accrued when a participant elects to join in the sharing framework. Once having joined, a jump can ensue: a participant may witness a doubling (i.e., $c = 2$) or even a tripling (i.e., $c = 3$) of their costs in order to sustain the framework as it goes through its perturbations of evolution. A participant’s acceptance of these cost-jumps reflect reluctance on the part of a participant to divest of the framework and thus lose their initial investment. Recognizing that participants would only embrace the framework because they might ultimately gain a benefit, the value assignment of $c = -2$ in Fig. 3.11 demonstrates the participant earning back its initial investment (of $c = 1$) together with an additional payback of the same amount. The aforementioned cost values depict a mix of favorable and unfavorable situations. Both types must be represented because professionals would recognize that inevitably both would be encountered in practice. Likewise, our values for the initial participating population ($\alpha_{\text{init}}$) are placed in the realm of reality. We assert that an outsider (that is a non-participant) cannot observe the sharing framework’s outcomes; instead they have to be in-situ to make meaningful determinations about the framework’s performance. Therefore, values of $\alpha_{\text{init}}$ are in the vicinity of 50% to indicate that about half of the initial population takes the optimistic approach (i.e., anticipates success) whereas the remaining part of the population tends toward the pessimistic (i.e., fears failure). These values are based on experience:
computer science is populated with protocols that can be either optimistic or pessimistic. For example, one can optimistically assume that deadlocks seldom occur and thus (hopefully) only have to rarely kill a deadlocked process; whereas, pessimistically, waits-for graphs are painstakingly constructed when a deadlock is fearfully anticipated - and subsequently - avoided. The choice to adopt an optimistic or pessimistic approach is based on finding a balance between performance expectations and risk, and in the evolution of computer science both types of approaches have consistently co-existed because that can be equally valuable. We therefore assigned $\alpha_{init}$ values that are near the pivotal balance between one of two choices. With a similar parameter selection approach, the nature of firms’ participation in CYBEX is derived with respect to different sharing costs ($x = 1, 2, \text{ and } 3$), which are depicted in Fig. 3.12 and 3.13. Since exchanging CTI comes at a non-zero cost, a participating organization may incur a unit cost ($x = 1$) or multiples of it, depending on the nature of the information involved and the consequences of sharing such CTI. The investment and incentive parameters are represented in the form of monetary quantities, hence their values can be straightforwardly chosen by the organization and CYBEX respectively (with appropriate normalization). As CYBEX evolves, we believe that real data will become available and that such data can be readily used to further verify our proposed model.

To verify our model for various values of $\alpha_{init}$ and sharing cost ($x$), an extensive set of simulation results are presented in Fig. 3.12 and Fig. 3.13. For the sake of generalization, we generate the results for two different values $\alpha_{init}$; (1) above 50%, where $\alpha_{init} = 0.65$ (2) below 50%, where $\alpha_{init} = 0.4$. The result set given in Fig. 3.12 represents the evolution of individuals taking participate strategy over stages, when the initial proportion of participants ($\alpha_{init}$) is 65% and CYBEX
imposes different participation costs ranging from $c = -2$ to 4. A similar simulation is conducted but with lesser initial participation, $\alpha_{init} = 0.4$, and the results are presented in Fig.3.13. It is observed that when cost of sharing is low ($x = 1, 2$) and firms are given incentives (i.e. $c < 0$), the population prefers the “Participate” strategy that eventually becomes ESS as seen in Fig.3.12a, Fig.3.12b, Fig.3.13a and Fig.3.13b irrespective of the initial population proportion. This is because, the condition (4) of our evolutionary analysis gets enforced here, where we know that “participate” strategy is evolutionarily stable. As $c$ increases to 1, the case (3) gets activated, where the required population threshold ($\alpha_{thres}$) is 0.37 when $x = 1$, 0.56 when $x = 2$, and 0.74 when $x = 3$. If we observe Fig.3.12a, where $\alpha_{init} = 0.65 > \alpha_{thres} = 0.37$, the population converges to complete participation and same happens in Fig.3.12b too $\alpha_{init} > \alpha_{thres} = 0.56$. However, in Fig.3.12c the population prefers not to participate because it did not have enough participants initially compared to $\alpha_{thres}$. We can now imagine that what situation will arise, when $\alpha_{init} = 0.4$. It is observed that the population will prefer to participate only when $x = 1$ because $\alpha_{init} = 0.4 > \alpha_{thres} = 0.37$ (Fig.3.13a) but not in any of the other two scenarios.

Now, when $c$ increases to 2, the case (3) is still valid and the required population threshold ($\alpha_{thres}$) is increased for $x = 1, 2, 3$ to 0.56, 0.74, and 0.93 respectively. Now for $\alpha_{init} = 0.65$, we can say that the only scenario when $x = 1$ will converge to “participate” stable strategy as shown in Fig.3.12a. However, when $x = 2, 3$, ‘No Participate” becomes ESS since $\alpha_{init} = 0.65 < \alpha_{thres}$. We can see that minimum participation threshold required for $x = 1, 2, 3$ is 0.56 which is more that $\alpha_{init} = 0.4$, none of the scenarios given in Fig.3.13 will converge to full participation.
Figure 3.12: Evolution of participating population w.r.t. participation and sharing cost, when initial participant proportion is 0.65
Figure 3.13: Evolution of participating population at different sharing cost, when initial participant proportion is 0.4
Chapter 3. *Self-Coexistence of Firms in CYBEX Framework*

When $c$ increases to 3, the case (3) will be valid only if $x \leq 2$, otherwise the cost component will dominate over the sharing gain and hence case (1) gets activated; which is why the population converges to “No Participate” strategy as shown in Fig.3.12c and Fig.3.13c. At $x = 1, 2$, required $\alpha_{\text{thres}} = 0.74$, and 0.93 respectively, which is more than $\alpha_{\text{init}}$. Hence the population converges to “No Participate” in Fig.3.12a, Fig.3.12b, Fig.3.13a, and Fig.3.13b for $c = 3$. When $c > 3$, the case (1) is applicable where ESS is “No Participate” strategy, as seen in Fig.3.12 and Fig.3.13 for $c = 4$.

### 3.4 Summary

In this Chapter, we have studied the problem of self-coexistence in CYBEX framework, i.e., how competing firms in a non-cooperative game can decide independently to participate in the CYBEX and share or not. We use evolutionary game theory to model the problem. Considering the cost of participation in CYBEX, in addition to the cost of sharing, we derived the conditions under which ESS can be achieved. We proposed a distributed learning heuristic which lead the firms towards ESS. We also demonstrate how CYBEX can wisely vary its pricing/incentive for participation by the firms to increase sharing which in turn increases its own revenue, eventually evolving toward a win-win situation.
Chapter 4

Evolutionary Game based
Information Sharing among Firms
in CYBEX Framework

4.1 Information Sharing Game

The above proposed game model best presents a scheme to motivate firms toward participating in CYBEX like sharing framework. Using evolutionary analysis, we derived conditional constraints on participation cost \( c \), a driving parameter for attracting firms to join and transact cyber-threat intelligence (CTI) with other firms. For the sake of simplistic analysis, we also assumed that every participating firm in CYBEX shares a constant amount of CTI. However, realistically some rational firms may share less whereas some share high based on their best interest. Hence constant sharing may not successfully capture the true sharing nature of firms, which is why we no longer restrain this assumption in
our extended model. As an extension, we address how the information exchange can be enhanced when firms differentiate their threat knowledge sharing nature after they participate in the framework. This is a very crucial problem because it can lead us to understand whether the firms truthfully intend to share all of their information or only exchange minimally to free-ride on others’ threat intelligence. In such cases, it is important to have different benefit components for differentiated sharing with additional exogenous support in terms of incentive from CYBEX to enhance and motivate the firms to truthfully share more cyber-threat information. To analyze this differentiated sharing scenario, we extend the evolutionary analysis for a strategic game called “differentiated information sharing game”, where players are mixture of firms participating in CYBEX and non-participants. The strategic form game of information sharing is discussed extensively in the following subsections.

4.1.1 Formulating Information Sharing Game

To measure advantages of information sharing from the perspective of participants compared to the ones who are not willing to participate in CYBEX, we considered mix of $N$ rational firms (both participants and non-participants) in the strategic game. For the sake of simplicity, we assumed that firms have three choices in the strategic game irrespective of their participation. If the firm is participating, it can either choose all of its discovered CTIs or choose to share less CTI than its potential or if it is not satisfied with the sharing benefits it can leave the framework and be a non-participant. Thus, from a firm’s perspective the objective is to find a stable equilibrium strategy among the three above discussed ones that will maximize the best interest of the firm, which is the CTI sharing
benefits. On the other hand, CYBEX is aiming to bring more firms to the sharing framework and lead them to share all of their CTIs truthfully rather than allowing the firms to free-ride. To do so, CYBEX introduces two different incentive parameters for two different sharing levels which we call as high sharing (HS) strategy and low sharing (LS) strategy. Now it is vital to investigate, under what conditions these incentives can bring the group of firms taking LS strategy to HS strategy so that every firm can truthfully share all of its threat knowledge in the community. To model the payoff of the firms, we have extended the components used in CYBEX participation game in the information sharing game.

4.1.1.1 Differentiated Sharing Gain

When a firm is not participating in the sharing framework, then we can infer that the firm is not interested in sharing its CTIs with others and decides to tackle cybersecurity issues solely. Therefore, these non-participants do not expect anything from CYBEX. However, some firms out of curiosity might want to get involved in the exchange framework to check whether they can resolve any security issues by exchanging a few information. This acute distinction between two actions made us to formulate two of the three strategies, i.e. no participation (NP) and low sharing (LS), for the information sharing game. However, there can be some firms who actually realized about the advantages of information sharing and are willing to share all of their information truthfully. This action of firms is denoted as high sharing (HS) strategy. LS strategy is only favorable in two scenarios, (1) when the firms do not get the worth of their truthfully shared cyber-threat information, (2) when firms decide not to share all of their information and free-ride on others’ CTIs, so that the cost of information sharing
is minimized. These cases motivated us to have only three strategies for the information sharing game which will also help in simplifying the evolutionary analysis of the game.

Since the firms have two choices of action for sharing their CTIs, the reward for both actions must be different. When the firms choose to share few information, i.e. take low share (LS) strategy, the reward for such action is directly dependent on strategy taken by the other interacting firm. Therefore, if the interacting firm is sharing less or fully sharing, then the gain for LS strategy will be low or high respectively. However, when a firm which shares information, interacts with a non-participating firm, then we assume that the sharing firm do not receive any benefit for its sharing rather incurs cost for such action. The rewards are nothing but the quantitative form of incidence responses, patches/fixes for vulnerabilities etc. In addition to the gain out of distinct sharing nature, the firms get benefited from their direct investment towards cybersecurity too.

4.1.1.2 Incentive Integrated Cost Component

It is clear that when a firm does not participate in the sharing framework, it does not share any of its threat intelligence, which is a risk averse and cost reduction strategy that might not be helpful in long-term. The firms who risk to participate and share information incur a cost for both participation as well as CTI exchange. The cost of CTI exchange might be due to risk of reputation loss or chances of getting flooded with attacks based on the shared vulnerabilities. Since the firms are participating in CYBEX, they can help out each other to recover from hazardous situations by sharing necessary threat related responses. So we integrate an incentive parameter from CYBEX that can waive some of
the cost incurred with firms’ participation and CTI sharing. The incentives are not necessarily same for HS and LS strategies rather have a strict difference. Incentive of minimal sharing cannot exceed the incentive for fully share strategy. However, these incentives can be wisely chosen by CYBEX to motivate firms to truthfully share all their CTIs.

4.1.2 Strategic Form of Information Sharing Game

In this subsection, we formulate the strategic form of the information sharing game. As per our above discussion, the players in this game have three strategies namely (i) High Sharing (HS) (ii) Low Sharing (LS) (iii) No Participation (NP). We consider that when the firms do not participate, they do not incur the cost of participation and also do not gain anything from information sharing. However, they only gain from their own investment. When the firms share low, which means they participate in the information sharing game, they incur a participation cost and the sharing cost at the same time while getting benefited not only from their sharing activity and investment but also externally from the CYBEX as incentives. The similar case happens when the firms share fully too, but the firm taking this strategy is assumed to gain more compared to the ones who choose low sharing strategy. As a matter of fact, if the incentives are not worthy enough, the firms always choose not to participate at all.

Once the game is formalized, it is our best interest to solve it from an evolutionary game point-of-view to define what strategies are evolutionarily stable and under what conditions they can be achieved. By saying equilibrium stable strategy (ESS) we are required to verify that no other population deviating from the ESS can completely invade the population playing with ESS strategy. Through such
analysis, we can come up with scenarios, where incentives from CYBEX can be controlled tactfully to avoid free-riding and at the same time firms can truthfully share all of their CTIs with each other. Assuming the strategy set $S_i$ for firm $i$ can be the following, Table 4.1 represents the strategic form of information sharing game, when a pairwise interaction among two firms occurs.

$S_i = \{ \text{High Sharing (HS), Low Sharing (LS), No Participation (NP)} \}$

<table>
<thead>
<tr>
<th></th>
<th>HS</th>
<th>LS</th>
<th>NP</th>
</tr>
</thead>
<tbody>
<tr>
<td>HS</td>
<td>$S_h a \log(1 + I) - x_h - c + \delta_1$</td>
<td>$S_a \log(1 + I) - x_h - c + \delta_1$</td>
<td>$a \log(1 + I) - x_a - c + \delta_1$</td>
</tr>
<tr>
<td>LS</td>
<td>$S_h a \log(1 + I) - x_l - c + \delta_2$</td>
<td>$S_l a \log(1 + I) - x_l - c + \delta_2$</td>
<td>$a \log(1 + I)$</td>
</tr>
<tr>
<td>NP</td>
<td>$a \log(1 + I) - x_h - c + \delta_1$</td>
<td>$a \log(1 + I) - x_l - c + \delta_2$</td>
<td>$a \log(1 + I)$</td>
</tr>
</tbody>
</table>

**Table 4.1: Strategic–form of Information Sharing Game**

We extended the similar game structure as we proposed for CYBEX participation game previously by integrating differentiated sharing gain/cost component and CYBEX controlled incentives. From Table 4.1, it can be seen that when two firms have decided to participate, their CTI sharing strategies can be distinguished into two categories: share minimally or fully share. If both firms choose to take the same strategies (either LS or HS), then their payoffs received are same because the gain and cost components are assumed to be same for same strategies.

However, when one firm takes LS strategy and other takes HS strategy, this situation can be classified as free-riding of the former firm. Since the firm playing LS strategy receives complete set of CTIs exchanged by the firm taking HS strategy, its indirect sharing gain is $S_h > 1$, whereas the truthful firm does not receive enough support from the other firm and ended up having a sharing gain of $S_l > 1$, where $S_h > S_l$. Thus to prevent such free-riding situations, external incentives $\delta_1, \delta_2$ from CYBEX are introduced. When CYBEX observes the firm’s truthful nature towards CTI sharing, it incentivizes $\delta_1$ otherwise a
lesser incentive of $\delta_2$ is awarded. These incentives keep the firms motivated toward information sharing, however incentives can tactfully be used to punish them if free-riding is detected. The cost component for a participating firm is composed of participation cost ($c$) and the sharing cost based on chosen strategy ($x_h$ for HS and $x_l$ for LS strategy). Since there is a clear distinction between high share and low share strategy in terms of quantity of information exchanged, the cost of taking such strategies is also ordered according to same metric. Thus we assume that $x_h > x_l$. When a participating firm interacts with a non-participant, it is clear that the non-participating firm cannot get advantages of CTI shared by the participating firm. Whereas if the participating firm shares less or high CTIs, a sharing cost of $x_l$ or $x_h$ will be incurred respectively but the non-participant does not incur any cost at all, not even participating cost and none of them gains anything in terms of threat intelligence.

### 4.2 Evolutionary Analysis of Information Sharing Game

To find the evolutionary stable strategy of the above formulated three-strategy game, we assume $p_1, p_2, p_3$ are the proportions of total $N$ population taking strategy HS, LS and NP respectively, where $p_1 + p_2 + p_3 = 1$. To understand the dynamics of firm population taking LS strategy and HS strategy, we derive the replicator equation for both population groups.

\[
g_1(p_1) = p_1(\mathbb{E}[U_{HS}] - \mathbb{E}[U_{net}]) \quad \text{(4.1)}
\]

\[
g_2(p_2) = p_2(\mathbb{E}[U_{LS}] - \mathbb{E}[U_{net}]) \quad \text{(4.2)}
\]
where, \( E[U_{HS}] \) and \( E[U_{LS}] \) are the expected payoff of a firm when it chooses “High Sharing” and “Low Sharing” strategy respectively, and \( E[U_{net}] \) is the average utility of the population of firms.

\[
E[U_{net}] = p_1 E[U_{HS}] + p_2 E[U_{LS}] + p_3 E[U_{NP}] 
\]  
(4.3)

\[
E[U_{HS}] = a \log(1 + I)(p_1 S_h + p_2 S_l + p_3) - x_h - c + \delta_1 
\]  
(4.4)

\[
E[U_{LS}] = a \log(1 + I)(p_1 S_h + p_2 S_l + p_3) - x_l - c + \delta_2 
\]  
(4.5)

\[
E[U_{NP}] = a \log(1 + I) 
\]  
(4.6)

Replacing the expected utility expressions from equation 4.3, 4.4, 4.5 in replicator dynamics equations 4.1 and 4.2, we find,

\[
g_1(p_1) = p_1 \{a \log(1 + I)(1 - p_1 - p_2)[p_1(S_h - 1) + p_2(S_l - 1)] - (x_h + c - \delta_1)(1 - p_1) + (x_l + c - \delta_2)p_2\} 
\]  
(4.7)

\[
g_2(p_2) = p_2 \{a \log(1 + I)(1 - p_1 - p_2)[p_1(S_h - 1) + p_2(S_l - 1)] + (x_h + c - \delta_1)p_1 - (x_l + c - \delta_2)(1 - p_2)\} 
\]  
(4.8)

Evolutionary stability for the information sharing game can be achieved when the following conditions are achieved: (1) the rate of change of different population proportions are zero, (2) neighborhood of the fixed points or possible stable strategies found must be also stable. Therefore, the replicator equation \( g_1(p_1) \) and \( g_2(p_2) \), a.k.a transformation speed of high sharing and low sharing population group must be equated to zero and solved to obtain the possible fixed points. Hence by solving \( g_1(p_1) = 0, g_2(p_2) = 0 \), and taking all possible
combinations of following expressions, we can find the set of possible solutions of $p_1$ and $p_2$.

$$p_1 = 0 \text{ or, } a \log(1 + I)(1 - p_1 - p_2)(p_1 S_h' + p_2 S_l') = \tilde{x}_h(1 - p_1) - \tilde{x}_l p_2 \quad (4.9)$$

$$p_2 = 0 \text{ or, } a \log(1 + I)(1 - p_1 - p_2)(p_1 S_h' + p_2 S_l') = -\tilde{x}_h p_1 + \tilde{x}_l(1 - p_2) \quad (4.10)$$

where, $\tilde{x}_h = x_h + c - \delta_1$, $\tilde{x}_l = x_l + c - \delta_2$, $S_h' = S_h - 1$, and $S_l' = S_l - 1$

Thus the set of solutions for triple $(p_1, p_2, p_3)$ can be listed as followings:

$$\alpha_{sol_1} = (0, 0, 1) \quad (4.11)$$

$$\alpha_{sol_2} = (0, 1, 0) \quad (4.12)$$

$$\alpha_{sol_3} = (0, \frac{\tilde{x}_l}{AS_l}, 1 - \frac{\tilde{x}_l}{AS_l}) \quad (4.13)$$

$$\alpha_{sol_4} = (1, 0, 0) \quad (4.14)$$

$$\alpha_{sol_5} = (\frac{\tilde{x}_h}{AS_h}, 0, 1 - \frac{\tilde{x}_h}{AS_h}) \quad (4.15)$$

Two more solutions can be found by solving the following two expressions from Eqn. 4.9 and Eqn. 4.10.

$$a \log(1 + I)(1 - p_1 - p_2)(p_1 S_h' + p_2 S_l') = \tilde{x}_h(1 - p_1) - \tilde{x}_l p_2$$

$$a \log(1 + I)(1 - p_1 - p_2)(p_1 S_h' + p_2 S_l') = -\tilde{x}_h p_1 + \tilde{x}_l(1 - p_2)$$

Since the l.h.s of both equations are same, we can equate the r.h.s expressions and by solving we can find that $\tilde{x}_l = \tilde{x}_h = x$. This condition will only be satisfied if $p_1 = p_2 = p$, hence the sharing gains must be same, i.e. $S_h' = S_l' = s$. Now
solving for one of the above equations including all the assumptions, we find

\[(1 - 2p)(2Asp - x) = 0\]

\[p = 0.5 \text{ or } p = \frac{x}{2As}\]

Thus, the new possible solutions triples can be

\[\alpha_{sol_6} = (0.5, 0.5, 0)\] (4.16)

\[\alpha_{sol_7} = \left( \frac{x}{2As}, \frac{x}{2As}, 1 - \frac{x}{As} \right)\] (4.17)

We found 7 possible solution triples as fixed points of the evolutionary game. However, we must check which of these solutions are in fact stable by verifying the neighborhood stability criteria.

### 4.2.1 Stability Verification of Fixed Points

According to Taylor and Jonker [97], a fixed point \( p = (p_1, p_2) \) is said to be strictly stable equilibrium strategy, if the eigen values [98] of \( J(g_1, g_2) \) matrix have negative real part, where \( J(\cdot) \) is the Jacobian matrix of replicator dynamics equations and represented by the following.

\[J(g_1, g_2) = \begin{bmatrix} \frac{\partial g_1}{\partial p_1} & \frac{\partial g_1}{\partial p_2} \\ \frac{\partial g_2}{\partial p_1} & \frac{\partial g_2}{\partial p_2} \end{bmatrix}\]

where, first order differentials are:

\[\frac{\partial g_1}{\partial p_1} = A(1 - 2p_1 - p_2)(p_1S'_h + p_2S'_l) + A_p(1 - p_1 - p_2)S'_h - (1 - 2p_1)x'_h + p_2x'_l\]
Chapter 4. Evolutionary Game based Information Sharing in CYBEX

\[
\frac{\partial q_1}{\partial p_2} = -Ap_1(p_1S_h' + p_2S'_l) - Ap_1(1 - p_1 - p_2)S'_l + p_1\tilde{x}_l \\
\frac{\partial g_2}{\partial p_2} = A(1 - p_1 - 2p_2)(p_1S_h' + p_2S'_l) + Ap_2(1 - p_1 - p_2)S'_l + p_1\tilde{x}_h - (1 - 2p_2)\tilde{x}_l \\
\frac{\partial g_2}{\partial p_1} = -Ap_2(p_1S_h' + p_2S'_l) - Ap_2(1 - p_1 - p_2)S'_l + p_2\tilde{x}_h
\]

Now, we are required to check which of the fixed points from \(\alpha_{sol_1}\) to \(\alpha_{sol_7}\), when imposed on the Jacobian matrix can produce an eigen vector that has negative real part. This mandatory check can take care of the neighborhood stability criteria. Now we derive the Jacobian matrix at each fixed point found previously (Eqn. 4.11 – 4.17) in the following:

\[
J_{\alpha_{sol_1}=(0,0,1)} = \begin{bmatrix} -\tilde{x}_h & 0 \\ 0 & -\tilde{x}_l \end{bmatrix} \quad (4.18)
\]

\[
J_{\alpha_{sol_2}=(0,1,0)} = \begin{bmatrix} -\tilde{x}_h - \tilde{x}_l & 0 \\ -AS_s' - \tilde{x}_h & -AS'_l + \tilde{x}_l \end{bmatrix} \quad (4.19)
\]

\[
J_{\alpha_{sol_3}=(0, \frac{\tilde{x}_l}{AS'_l}, 1 - \frac{\tilde{x}_l}{AS'_l})} = \begin{bmatrix} \tilde{x}_l - \tilde{x}_h & 0 \\ J_{11} & \tilde{x}_l(1 - \frac{\tilde{x}_l}{AS'_l}) \end{bmatrix} \quad (4.20)
\]

\[
J_{\alpha_{sol_4}=(1,0,0)} = \begin{bmatrix} -AS_s' + \tilde{x}_h & -AS'_l - \tilde{x}_l \\ 0 & -\tilde{x}_h - \tilde{x}_l \end{bmatrix} \quad (4.21)
\]

\[
J_{\alpha_{sol_5}=(\frac{\tilde{x}_l}{AS'_l}, 0,1 - \frac{\tilde{x}_l}{AS'_l})} = \begin{bmatrix} \tilde{x}_h(1 - \frac{\tilde{x}_l}{AS'_h}) & J_{12} \\ 0 & \tilde{x}_h - \tilde{x}_l \end{bmatrix} \quad (4.22)
\]

\[
J_{\alpha_{sol_6}=(0.5,0.5,0)} = \begin{bmatrix} \frac{-A}{4}(S_h' + S_l') + \frac{\tilde{x}_l}{2} & \frac{-A}{4}(S_h' + S_l') + \frac{\tilde{x}_l}{2} \\ \frac{-A}{4}(S_h' + S_l') + \frac{\tilde{x}_h}{2} & \frac{-A}{4}(S_h' + S_l') + \frac{\tilde{x}_l}{2} \end{bmatrix} \quad (4.23)
\]

\[
J_{\alpha_{sol_7}=(\frac{\tilde{x}_l}{AS'_l}, \frac{\tilde{x}_l}{AS'_l}, 1 - \frac{\tilde{x}_l}{AS'_l})} = \begin{bmatrix} 0.5x - \frac{x^2}{2As} & -0.5x + \frac{x^2}{2As} \\ -0.5x + \frac{x^2}{2As} & 0.5x - \frac{x^2}{2As} \end{bmatrix} \quad (4.24)
\]
We now need to verify which of the fixed points are stable according to neighborhood stability criteria. Therefore, we need the eigen values of the Jacobian matrix derived earlier must have negative real part [97]. To find the eigen values (\( \lambda \)) of a matrix \( A \), we must solve the equation \( \det(A - \lambda I) = 0 \), where \( \lambda \) denotes the eigen values of matrix \( A \) and \( I \) represents the identity matrix of same dimension as \( A \). In the following, we find the eigen values of the Jacobian matrix at each fixed point and the conditions at which the stability can be achieved.

1. Eigen values of \( J|_{\alpha_{sol1}} \) are \( \lambda_1 = -\tilde{x}_h \) and \( \lambda_2 = -\tilde{x}_l \), which have negative real part if the following conditions are satisfied.

\[
\delta_1 < x_h + c \quad \text{and} \quad \delta_2 < x_l + c
\]  

(4.25)

2. Eigen values of \( J|_{\alpha_{sol2}} \) are \( \lambda_1 = -\tilde{x}_h - \tilde{x}_l \) and \( \lambda_2 = -AS'_l + \tilde{x}_l \). The eigen values are real by themselves and they can be negative if the following conditions are held.

\[
\delta_1 + \delta_2 < x_h + x_l + 2c \quad \text{and} \quad \delta_2 > x_l + c - A(S_l - 1)
\]

\[
\implies x_l + c - A(S_l - 1) < \delta_2 < (x_h + x_l + 2c) - \delta_1 \quad (4.26)
\]

and \( \delta_1 < x_h + A(S_l - 1) \)  

(4.27)

3. Eigen values of \( J|_{\alpha_{sol3}} \) are \( \lambda_1 = \tilde{x}_l(1 - \frac{\tilde{x}_l}{AS'_l}) \) and \( \lambda_2 = -\tilde{x}_h - \tilde{x}_l \). From the fixed point \( \alpha_{sol3} = (0, \frac{\tilde{x}_l}{AS'_l}, 1 - \frac{\tilde{x}_l}{AS'_l}) \), it is clear that \( \frac{\tilde{x}_l}{AS'_l} \leq 1 \) and \( \tilde{x}_l > 0 \). Hence the eigen value \( \lambda_1 \) cannot be negative. Therefore, the solution \( \alpha_{sol3} \) is not a
stable equilibrium. By similar reasoning, we can also prove that the fixed point \( \alpha_{sol_5} \) is not a stable strategy.

4. Eigen values of \( J|_{\alpha_{sol_4}} \) are \( \lambda_1 = -\bar{x}_h - \bar{x}_l \) and \( \lambda_2 = -AS'_h + \tilde{x}_h \). The eigen values are real and they can be negative if the following conditions are satisfied.

\[
\delta_1 + \delta_2 < x_h + x_l + 2c \quad \text{and} \quad \delta_1 > x_h + c - A(S_h - 1)
\]

\[
\implies x_h + c - A(S_h - 1) < \delta_1 < (x_h + x_l + 2c) - \delta_2 \quad (4.28)
\]

and, \( \delta_2 < x_l + A(S_h - 1) \quad (4.29) \)

5. Finding the eigen values of \( J|_{\alpha_{sol_5}} \) leads to solve the following equation

\[
\lambda \left( \lambda + \frac{-A}{2}(S'_h + S'_l) - \frac{\tilde{x}_h + \tilde{x}_l}{2} \right) = 0
\]

It is clear that one of the eigen values is zero, which by itself invalidates the stability criteria. Therefore the fixed point \( \alpha_{sol_5} = (0.5, 0.5, 0) \) is not a stable equilibrium. Using the similar analysis on \( J|_{\alpha_{sol_6}} \), we can find that one of the eigen values is zero. Since it cannot be negative, we simply discard this unstable solution.

After analyzing the above scenarios, we conclude that each of the three strategies has potential to be an evolutionarily stable strategy for the firms. However, the decision of a particular ESS can be controlled by the incentive parameters guided by CYBEX. In other words, we can state that the CYBEX controlled incentive parameters \( \delta_1, \delta_2 \) can be suitably altered so that one of the desired scenario can be achieved. The incentive parameters can essentially be used to motivate the
firms taking LS strategy towards sharing all of their information truthfully, i.e. adopting HS strategy.

4.3 Results and Discussion

To demonstrate that different stable equilibrium strategies can be achieved for the information sharing game, we conduct some simulations by considering a population of size 100. Throughout the experiments, we fix a unity rationality constant ($a$) and investment ($I$) of 15. The sharing gain parameters of HS and LS strategies are assumed to be 3 and 1 units respectively. The participation cost is taken as 2 units. The sharing costs for HS and LS are considered as 5 and 3 units respectively. In such scenario, if the incentives $d_1$ and $d_2$ are taken in such a way that the $\tilde{x}_h, \tilde{x}_l$ are positive, the stable equilibrium strategy will be not to participate. This situation is shown in Fig. 4.1 and it can be observed that even if the population proportion of all three different strategies are same in the beginning, the participating firms are invaded by the non-participating firms. Eventually all the firms decide not to participate as the average utility reward out of sharing is not benefiting sufficiently.

In some situations, CYBEX might be interested in motivating firms to start sharing some of their CTIs, which may not be maximal. Thus the incentive for LS strategy $\delta_2$ can be suitably increased to grow the population towards LS strategy. In the plot given in Fig. 4.2, we can see that when incentive $\delta_2$ is increased to 7, the population from no-participant group and high sharing group got invaded easily, leaving the LS strategy as evolutionary stable strategy. On the other hand, if the incentive for high sharing is increased by CYBEX, then every firm prefers
to be in HS group due to higher reward However, when sufficient firms have switched their strategy to share completely and truthfully, the incentive of HS strategy can be reduced. A sample simulation scenario is presented in Fig. 4.3,
where we can observe that the population of HS strategy group could easily invade other populations when the external incentive is increased to 5. Thus we can conclude from these three instances that the incentive parameters are crucial guiding parameter that can decide which strategy can be evolutionarily stable and it can be easily exploited by CYBEX to enable every firm to participate and share their CTIs truthfully.

4.4 Summary

In this Chapter, we have formulated an information sharing game, and analyzed using evolutionary dynamics. We observed that the external incentivization from CYBEX can motivate the firms to share more information truthfully instead of staying out of the sharing framework or sharing minimally. We analyzed the
game and lay out the various possible stable strategies (pure and mixed). It is shown that not all of the solutions passed the neighborhood stability criteria, but only three solutions came out as evolutionary stable strategies (ESS) under certain conditions on incentive parameters. The conditional constraints can provide a mechanism for CYBEX to enforce the firms for sharing all of their cybersecurity information truthfully by adopting “high sharing” strategy.
Chapter 5

Non-Cooperative Game Model on Cyber-Threat Information Sharing

In this Chapter, we model the threat-intelligence information sharing as a distributed and non-cooperative game among $N$ firms and propose an incentive framework to foster their information sharing behavior. Such exchange process helps every firm to boost its security, which is modeled as incentive from the framework, but it costs the firm too in terms of market value and reputation etc. This trade-off has been considered for formulating a robust utility model that is scalable to any number of firms, to reward them based on their information sharing and willingness to invest. Since the firms’ net benefit is not only driven by their own security investment and sharing intentions, but also on other firms’ decision parameters, individual benefit maximization requires every firm to play with their best-response strategy so that socially optimal equilibrium can be achieved. Therefore, it is necessary for the firms to find their best response investments and information sharing amount from a firm’s perspective, which
will optimize their net reward. We now model our problem and later deduce the general condition under which a socially-optimal solution could be achieved.

## 5.1 System Model and Game Formulation

We consider a market scenario, where $N$ firms are playing in this game aiming to strengthen their cybersecurity infrastructure via security investments and breach/patch related information sharing. Without loss of generality, we assume that each firm $i$ invests $I_i \in [0, 1]$ amount of its total annual investment budget towards security development and decides to share $l_i \in [0, 1]$ amount of the total breach/patch related information with other firms at a decision point.

### 5.1.1 Security Information Exchange Game

The security information exchange game, $G = (N, S, U)$ is played in a distributed manner among the $N$ firms, where $i^{th}$ firm has two variable continuous strategy space $S_i = \{(I_i, l_i) : l_i \in [0, 1], I_i \in [0, 1]\}$. To compensate the cost of information loss due to successful cyber crime and defend future cyber attacks, the firms (1) consider monetary investment for further advancements in security, and (2) share the vulnerability information set with other firms or central information exchange for collaborative effort. The rational entities face the optimization problem to find the best response strategy of maximizing overall payoff where, cost of both security investment and information sharing of the firm is minimized. The strategy profile, $s = \{s_1, s_2, ..., s_N\} \in \hat{S}$, constitutes set of individual strategies for networks $1, 2, ..., N$ where, $\hat{S} = S_1 \times S_2 \times ... \times S_N$. By taking strategy $S_i$, the
firm decides to exchange $l_i$ amount of vulnerability information and invests $I_i$ amount towards security technology.

The devised utility equation incentivizes the firms for better contribution to the information exchange framework and the firms are expected to figure out the corresponding equilibrium strategies that maximize their overall payoff. Using cost-benefit approach, the utility expression for the game $G$ is formulated which considers sharing gain, cost of security investment, relative cost of security information exchange, and cost of processing the collected information. In practice, many other cost and benefit components like stock value, market reputation, customer satisfaction ability can be considered in incentivizing a firm to bolster security information sharing. But for the sake of tractable analysis of the proposed game theoretic model, we consider the four above discussed major components in this work, which are briefed in the following subsections.

### 5.1.2 Sharing and Investment Gain

In addition to the direct benefits from a firm’s own investment, it also receives indirect gain from other firms’ shared information on vulnerability patches and fixes. So the overall gain to a firm not only depends on own security investment, but also on the other firms’ sharing intentions, and their investment levels. To model the indirect gain from other firms, we assumed a quadratic function to measure the benefits of shared information from every other firm. However, any increasing function instead of quadratic can also be applied to model the information sharing benefits. A logarithmic gain function $G_i$ for firm $i$ is considered to model the total utility gain from overall direct investment and
indirect sharing benefits.

\[ G_i(S_i, S_{-i}) = f(N) \log \left( I_i + \sum_{j \neq i}^{N} \beta_{ij}(I_j + \tau \sum_{k \neq j}^{N} I_k^2) \right) \] (5.1)

The logarithmic gain function motivates the players by returning high reward at small steps towards information sharing and security investment. However, the reward saturates at high value of investment and information sharing, which explains that high investment does not necessarily increase the overall utility, rather reducing the investment level and increasing sharing level will return similar reward incurring less cost.

The scaling parameter \( \tau \) scales the investment and total value of competing firms’ shared information to equivalent dimension, and the parameter \( \beta_{ij} \) represents the conversion parameter that maps the usefulness of firm \( j \)'s shared information based on firm \( i \)'s security requirement. The value of \( \beta_{ij} \) becomes zero, when firm \( j \) does not share any security related information with firm \( i \). \( f(N) \) represents the gain scaling function of number of participants in the information exchange game, which helps to incentivize the players more when the number of participants in the game increases. Therefore, more firms will be attracted to share their security information, which will eventually enhance the individual gross utility.

### 5.1.3 Cost of Security Investment and Information Exchange

The process of combating current/future cyber attacks requires help from other competing firms as well as monetary investment towards firm’s own security task force. The help-seeking firm is less likely to receive any vulnerability related
information or preventive mechanisms from other experienced firms until it exchanges its own breach/patch related information with others. However, this security information exchange is associated with the risk of tarnished reputation along with its market value, and customer base. In this work, the information sharing enabled cyber defense approach of a firm involves three types of cost parameters: (1) direct monetary cost for own security investment $C_T(I_i)$, (2) cost of information sharing $C_S(l_i, l_{-i})$, which is relative to other firms’ sharing intentions ($l_{-i}$), and (3) processing cost $C_P(l_{-i})$ of the received security information from other firms excluding $i$. The total cost to firm $i$ can be expressed as:

$$C_i(I_i, l_i, l_{-i}) = \theta_1 C_T(I_i) + \theta_2 C_S(l_i, l_{-i}) + \theta_3 C_P(l_{-i})$$

(5.2)

where, $0 \leq \theta_1, \theta_2, \theta_3 \leq 1$ are the scaling constants emphasizing the cost of investment and information sharing respectively.

Intuitively, the investment cost function, $C_T(I_i)$ must increase when firm $i$ increases its security investment $I_i$, i.e. $\frac{\partial C_T}{\partial I_i} > 0$. The cost of information sharing $C_S(.)$ increases as firm $i$ increases its information sharing level, i.e. $\frac{\partial C_S}{\partial l_i} \geq 0$. However, this information sharing cost is relieved, when every firm simultaneously exchanges its security information with each other, because the customers perceive this action as a positive step towards defending against cyber crimes. Hence the firm’s market value, customer satisfaction, and reputation is likely to be unaffected when everybody support security information exchange, i.e. $\frac{\partial C_S}{\partial l_j} \leq 0$, $\forall j \neq i$. The example cost function of information sharing given in Eqn. 5.3 satisfies the above-mentioned properties, which is a sum of relative sharing intentions times total shared information in the interaction, with respect to every other firm.
Chapter 5. Non-Cooperative Game Model on CTI Sharing

To retrieve the best out of the collected security information from different firms, it is required to filter out the relevant information and process them according to firm $i$’s requirements. This requires an extra effort and cost to be invested for effective utilization of the collected information, thus the cost of information processing can be expressed in Eqn. 5.4.

\[
C_S(l_i, l_{-i}) = \sum_{j \neq i} (l_i + l_j)(l_i - l_j) = \sum_{j \neq i} (l_i^2 - l_j^2) \quad (5.3)
\]

\[
C_P(l_{-i}) = \sum_{j \neq i} \gamma_{ij} l_j \quad (5.4)
\]

where, $\gamma_{ij} \in [0, 1]$ represents the firm $i$’s processing overhead to extract out and process the useful information from the firm $j$’s ($j \neq i$) shared information set.

5.2 Optimization Problem

The cost-benefit analysis of information exchange game requires to find the best response values of decision variables such as investment and sharing level. The firms suitably change the values of their decision parameters to optimize its net utility, however this cannot be achieved without cooperation of other firms. It is expected that the proposed incentive mechanism will self-enforce security information sharing among the participating firms which in turn will reduce the investment costs of individual participants. Also, when the number of firms involved in the game increases and they truthfully exchange their vulnerability information, the overall gain is improved at minimal cost for information sharing. The unconstrained optimization problem of choosing best response investment and sharing level decision can be found by maximizing the
Chapter 5. Non-Cooperative Game Model on CTI Sharing

objective function given in Eqn. 5.5, which is formulated by combining the gain and cost components from Eqn. 5.1 and Eqn. 5.2 respectively.

Maximize 
\[ U_i(S_i, S_{-i}) \]
\[ = f(N) \log \left( I_i + \sum_{j \neq i} \beta_{ij}(I_j + \tau \sum_{k \neq j} l_{ik}^2) \right) \]
\[ - \theta_1 C_T(I_i) - \theta_2 ((N - 1)I_i^2 - \sum_{j \neq i} l_{ij}^2) - \theta_3 \sum_{j \neq i} \gamma_{ij} l_j \]
(5.5)

5.2.1 Best Response Analysis

The objective function presented in Eqn. 5.5 needs to be maximized with respect to a firm’s security investment \( (I_i^*) \) as well as sharing intention level \( (l_i^*) \), assuming other players keep their investment and sharing intentions as their best responses. Hence, for finding \( I_i^* \),
\[ \frac{\partial U_i(\cdot)}{\partial I_i} = f(N) \frac{Z}{Z} - \theta_1 C_T'(I_i) = 0 \]
(5.6)
Assuming \( Z = I_i + \sum_{j \neq i} \beta_{ij}(I_j + \tau \sum_{k \neq j} l_{ik}^2) \), the following needs to be computed,
\[ \frac{\partial^2 U_i(\cdot)}{\partial I_i^2} = -f(N) \frac{Z^2}{Z^2} - \theta_1 C_T''(I_i) \]
(5.8)

Assuming \( I_i = I^* \) is the best response investment level, then the following open form equation must be satisfied.
\[ I_i^* = \frac{f(N)}{\theta_1 C_T''(I_i^*)} - \sum_{j \neq i} \beta_{ij}(I_j + \tau l_{ij}^2) \]
(5.7)
From Eqn. 5.8, it is clear that \( \frac{\partial^2 U_i}{\partial l_i^2} < 0 \), provided \( C''_T(I_i) > 0 \) and for positive value of investment, \( \frac{f(N)}{\delta C'_T(I_i)} > (\sum_{j \neq i} \beta_{ij}(I_j + \tau \sum_{k \neq j} I_k^2)) \) must be satisfied.

To promote security information sharing, the firms should be rewarded more with increase in their sharing intentions. Thus, the best response value of \( l_i \) should be the maximum value that it can take, and the gross utility of firm \( i \) presented in Eqn. 5.5, must be an increasing function w.r.t \( l_i \), when the investments and sharing intentions of other firms are constant. The condition presented in theorem 5.2.2 must be satisfied to self-enforce the firms to share their security information.

**Definition 5.2.1.** A continuous function \( f(x) \) is said to be increasing in the interval \([a, b] \), if its first order differential \( f'(x) \) is positive \( (f'(x) > 0) \) between the given interval.

**Theorem 5.2.2.** The gross utility function \( U_i(.) \) increases with respect to firm \( i \)'s sharing intention in the range \( \{(l^1_i, l^2_i) : l^1_i < l^2_i\} \) provided the following condition is satisfied.

\[
\frac{Z(l^1_i)Z(l^2_i)}{I_i + \sum_{j \neq i} \beta_{ij}(I_j - \tau l^1_i l^2_i)} < \frac{2f(N)\tau \sum_{j \neq i} \beta_{ij}}{2\theta_2(N - 1)}
\]

**Proof:** For proving the increasing nature in range \( (l^1_i, l^2_i) \), where \( l^1_i < l^2_i \) it is required to show that,

\[
\frac{\partial U_i(.)}{\partial l_i} \bigg|_{l^2_i} - \frac{\partial U_i(.)}{\partial l_i} \bigg|_{l^1_i} > 0
\]

\[
\frac{\phi_1 l^2_i}{\phi_2 + \phi_3(l^2_i)^2} - \frac{\phi_1 l^1_i}{\phi_2 + \phi_3(l^1_i)^2} > 2\theta_2(N - 1)(l^2_i - l^1_i)
\]

\[
\frac{\phi_1(\phi_2 - \phi_3(l^1_i)^2)}{(\phi_2 + \phi_3(l^1_i)^2)(\phi_2 + \phi_3(l^2_i)^2)} > 2\theta_2(N - 1)
\]

\[
\frac{Z(l^1_i)Z(l^2_i)}{I_i + \tau \sum_{j \neq i} l^2_j + \sum_{j \neq i} \beta_{ij}(I_j - \tau l^1_i l^2_i)} < \frac{\phi_1}{2\theta_2(N - 1)}
\]

(5.9)
where, \( \phi_1 = 2f(N) \tau \sum_{j \neq i} \beta_{ij}, \phi_2 = I_i + \sum_{j \neq i} \beta_{ij}(I_j + \tau \sum_{k \neq j,i} I_k^2), \phi_3 = \sum_{j \neq i} \beta_{ij} \tau. \)

Remarks: The above proved condition ensures that the firms will have higher benefits if they share more breach related information among each other. Hence, this condition helps to self-enforce the firms to participate in the sharing framework and share as much information as they can. Thus, it will (in)directly return a high utility reward to the firms and they can reciprocate the same behavior of exchanging security information to eventually reach an equilibrium state.

### 5.3 Results and Discussion

We studied the nature of the information sharing framework via numerical analysis and simulations to show that the firms can be benefitted more via breach/patch related information exchange. We present the results from static single stage analysis of the incentive model for two and more than two participating firms \((N = 2, 4, \text{ and } 20),\) where the overall utility rewards are reported by varying their information sharing intentions as well as investment levels. We assume that 80% of the collected shared information are useful for each firm, so \( \beta_{ij} \) is set to be 0.8. As the investment cost function \( C_T(I_i) \) presents the monetary cost of a firm towards security investment, we assume a quadratic function, where low investments return low cost but high investments increase the cost \( C_T \) rapidly. This factor can motivate the firms to participate in information exchange instead of making large security investments while defending cyber crimes. To promote information sharing, we consider a quadratic gain scaling function \( f(N) = aN^2 + bN + c : a, b, c \in \mathbb{R}, \) which triggers high reward when a large number of firms join the information exchange framework. However,
the nature of gain scaling function is not limited to only quadratic, rather any strictly increasing function of $N$ can be a candidate $f(N)$.

In Fig. 5.1, and 5.2, we studied the nature of overall utility variation with respect to firm $i$’s security investment levels by varying its information sharing intentions in a two-firms and 20-firms market scenario respectively. In this scenario, it is assumed that all other firms keep their investment level to 0.5 and fully share their security breach/patch information, i.e. $I_j = 1\forall j \neq i$. When firm $i$ increases its information sharing intention as well as it is willing to invest, we observe that there exists a best response investment level beyond which the investment cost dominates over the total gain. The best response value of investment apparently reduces as firm $i$ increases its information sharing limit irrespective of other firms’ actions. On another note, it can be stated that when the firm $j$ truthfully shares its information, firm $i$ cannot maximize its utility reward until it increases its information sharing level. Hence, the firms are required to self-enforce themselves towards information sharing to receive high payoff. To study the scalability of the framework, the same characteristics is experimented when $N = 20$ firms participate and it is observed that the gross utility to the considered firm is increased whereas the best response investment level representing the maximum utility is reduced compared to scenario of less number of participating firms. Therefore, the framework attracts more firms to participate in information sharing activity to receive maximum payoff.

In Fig. 5.3, we present the effect of other firms’ sharing levels on firm $i$’s utility reward with respect to $i$’s own security investment level, when the number of participating firms ($N$) is 4. Assuming two firms simultaneously change their information sharing levels from 0 to 1 with an increment of 0.25, it is
Chapter 5. Non-Cooperative Game Model on CTI Sharing

**Figure 5.1:** Optimal Investment on own sharing level variation \((N = 2)\)

**Figure 5.2:** Optimal Investment on own sharing level variation \((N = 20)\)
observed that when other firms do not share anything, the reward to the firm i is minimal. But we have seen from Fig. 5.1 that the firms who decrease their sharing limits, suffer with low utility reward. Hence, no single firm can gain more by reducing its information sharing limit, which self-enforces the rational firms to share more information to maximize their individual utility as well as system utility. Assuming 50% of the total participating firms fix their investment and sharing level to 0.5 and 1 respectively, Fig. 5.4 presents the behavior of total utility value to a firm when number of participating firms vary from 10 to 20. It is observed that the utility value increases with growing rate of participants in the exchange framework when they share maximally irrespective of other firm’s sharing intentions. Therefore, the framework can adapt high number of participants and self-enforce the firms to exchange more by rewarding high payoffs.

Fig. 5.5 presents the utility reward to firm i, when it unanimously changes its level of information exchange. We experimented to find how firm i’s security investment affects its overall received utility by varying its sharing level. It is clear from the plot that sharing more information can drive them to achieve high reward. Hence the profit-seeking firm i should always choose to share maximally with $l_i = 1$. Another point can be noted that minimum investment rewards minimum utility, however, a firm can improve its received reward gain by increasing its information sharing activity. Hence, the firms need to both invest a non-zero amount, and voluntarily share their vulnerability related information with other firms to receive maximum utility.

Fig. 5.6 and 5.7 show the utility variation when some firms decrease their security investments and try to free-ride on the other firms’ shared information for cases
Chapter 5. Non-Cooperative Game Model on CTI Sharing

FIGURE 5.3: Effect of others’ sharing level on Firm i’s investment

FIGURE 5.4: Utility vs. Number of participating firms
Chapter 5. Non-Cooperative Game Model on CTI Sharing

**Figure 5.5:** Effect of Firm i’s sharing level on received utility w.r.t. own investment level variation ($N = 4$)

**Figure 5.6:** Effect of Firm i’s sharing level on received utility w.r.t. other firms’ investment level variation ($N = 4$)
Chapter 5. Non-Cooperative Game Model on CTI Sharing

![Figure 5.7: Effect of Firm i’s sharing level on received utility w.r.t. other firms’ investment level variation ($N = 20$)](image)

of $N = 4$ and $N = 20$ respectively. It can be observed that when a firm $j(\neq i)$ reduces its security investment level then the overall utility of firm $i$ is negatively affected. As per the simulation conditions, majority of the participating firms are sharing their security information, hence firm $i$ can compensate the utility loss by increasing its information sharing level. From the previous results, we have seen that no firm can improve its payoff by making low security investment, hence the firms may not choose to free-ride by making very minimal investment or minimal information sharing due to the possibility of getting penalized with low utility reward. In the reported plot, we have showed that the reward value decreases when only one of the competing firms reduces its investment level, keeping its sharing intention high. It can be easily inferred that the reward value will be even lesser, when many firms will make minimal investment and
information sharing. Fig. 5.7 is reported to show that the behavior of framework remains unchanged even when the number of participating firms rises. Hence the framework can effectively self-enforce every firm to maximally share its breach/patch related information.

5.4 Summary

In this Chapter, we have modeled a simultaneous information exchange game and proposed an incentive framework by considering positive and negative aspects of breach/patch information sharing and security technology investment. The incentive model is verified via numerical analysis under scenarios of varying investment levels, and sharing intentions of the considered firms as well as from competing firms’ perspective. It is found that firms are incentivized more when they share more information among each other and firms’ security investments additionally help to maximize the received utility. The sharing nature also helps the firms in reducing their cost of investment in the long run too.
Chapter 6

Cyber-Investment and Cyber-Information Exchange Decision Modeling

Considering CYBEX provides a secure medium to share the threat information, we assume that it collects the shared information from each participating firm and forwards the aggregated information back to all participants. It also helps to motivate and self-enforce the firms towards sharing activity by using appropriate incentivization mechanism. Considering the challenges of information exchange process, in this chapter we formulate a simultaneous non-cooperative game-theoretic model to resolve the conflict of deciding how much security investment, a firm has to make, and how much threat information to share with CYBEX, such that its expected benefit is maximized.
Chapter 6. Cyber-Investment and Cyber-Information Exchange Modeling

6.1 System Model

A simultaneous game between the \( N \) competing companies is considered where CTI is exchanged through CYBEX. The corporations’ strategies are twofold: investment, and cyber-threat information exchange, where the technology investment helps them to conduct more research on the possible security breaches and the exchange strategy helps to reciprocate the sharing nature of others. The framework requires all participants to exchange their findings with CYBEX so that everyone else can get the most benefits in terms of information on vulnerabilities, loopholes, bugs, fixes, corrupted programs etc. It is assumed that the firms have a maximum budget of \( B \) to invest for security, and total \( L \) amount of information to share. A firm’s security investment is assumed to benefit only itself, however the received information helps both at the same time. Hence there is a possibility for some firms to free-ride on others information set, which must be prohibited to have a strategy-proof framework. CYBEX takes part in rewarding/punishing the firms based on their sharing attitude via an incentive model.

6.1.1 Game Formulation

Assuming \( N \) corporations, denoted by \( \mathcal{N} = \{1, 2, ..., N\} \), are participating in CYBEX information sharing framework, where firm \( i \in \mathcal{N} \) has a total budget of \( B_i \) to invest on security and \( L_i \in \mathbb{N} \) amount of cyber-threat related information, the strategy space of player \( i \) can be given as:

\[
S_i = \{(I_i, l_i) \in (B_i \times L_i) : 0 \leq I_i \leq B_i \text{ and } 0 \leq l_i \leq L_i \}
\]
Chapter 6. Cyber-Investment and Cyber-Information Exchange Modeling

CYBEX collects the information set $L = \{l_1, l_2, \ldots, l_N\}$ from $N$ participants and forwards the aggregated information set $(L_{-i})$ to every firm $i \in \mathcal{N}$, which helps in improving the robustness of firm $i$, characterized by $\mathcal{F}(L_{-i})$. After receiving the aggregated information set from CYBEX, the firms evaluate the effectiveness of the played strategies through a payoff function $U$, described later.

In the above described game $G(\mathcal{N}, S, U)$, we consider the generic abstraction of “always rational and profit-seeking” CYBEX as well as firms. The conflict of the corporations in the game can be described as follows: the firms always look for securing their systems with minimum investment and sharing few/no CTI with CYBEX. However, low investment may not help in discovering/fixing the security issues, thus information sharing activity with CYBEX also goes down. This cost-saving instance might not benefit the firms at all, rather worsen the security issues. On the other hand, if they make very high investment and fully share, then the firms might not afford such a high cost in terms of monetary and market value. Therefore, the corporations must choose their investments and amount of information to share very carefully so that their net benefit will be maximized. To fulfill the best interest of CYBEX, it aims to motivate as many participants to join in the framework and truthfully share their information, which will self-enforce other corporations to behave in similar way. In the next subsection, we model the firm’s payoff function using a cost-benefit approach.

### 6.1.2 Utility Formulation

In this subsection, we model the firms’ payoff, using several components described in the following.
Chapter 6. Cyber-Investment and Cyber-Information Exchange Modeling

6.1.2.1 Sharing and Investment Gain

If firm $i$ decides to make a positive investment and share its CTI with CYBEX, then it can receive two kinds of benefits: (1) direct gain from self-investment ($f_I(I_i)$) (2) robustness benefits from information sharing ($F(L_{-i})$). The former gain, out of investment $I_i \leq B_i$, can be defined as discovering various threat attributes, system loopholes, developing patches/fixes etc. The other firms’ shared information contributes as indirect gain in terms of firm $i$’s security robustness, which is represented by $F(L_{-i})$. $F$ is a function of total information shared in the system except the considered firm’s contribution and it is assumed that the robustness increases as the system’s information sharing activity rises.

The other factor, so called external incentive from CYBEX ($\alpha_i$), also has an important role in the gain component. This external benefit aims to self-motivate the firms initially towards sharing more, but as the firms are self-enforced this incentive fades away gradually. The net benefit out of $\alpha_i$ is scaled up with respect to the amount of firm $i$’s shared information ($l_i$) to provide the incentive in proportion to its information sharing activity. Assuming $\psi(l_i)$ is the sharing effectiveness function to reward a firm externally based on its nature of sharing, the gain from sharing can be expressed as:

$$G(S_i, S_{-i}) = (\alpha_i \psi(l_i) + F(L_{-i}))f_I(I_i) \quad (6.1)$$

The typical characteristics of investment gain function ($f_I(I_i)$) can be the following: the firms can benefit at a higher rate until certain investment, however making an investment beyond this threshold limit does not reward much. Thus it can be modeled as a variant of logarithmic function [99] similar to $\log(1 + I_i)$. For rationality constraint, $\log(1 + I_i) > 0$, otherwise the firms would never invest.
Chapter 6. Cyber-Investment and Cyber-Information Exchange Modeling

This gain saturates after a threshold and does not necessarily reward at a high rate. Assuming a linear sharing effectiveness function, the joint gain out of investment and CTI exchange can be expressed as:

$$G(S_i, S_{-i}) = a_0(\alpha_i l_i + \mathcal{F}(L_{-i})) \log(1 + I_i)$$  \hspace{1cm} (6.2)

where, $a_0 > 0$ is a simple scaling parameter that maps user satisfaction/benefit to a dimension of the price/monitory value. The external incentive parameter $(\alpha_i)$ is crucial from the CYBEX’s perspective, because it is modeled to motivate the firms towards sharing their CTI when the system of participants have not tasted the worth of this CTI exchange. However, when everyone is actively participating and sharing, then the incentive should fade away to let the sharing system self-sustained. In case of free-riding, the firm must be punished and no incentive should be given, so that the non-cooperation will be avoided. Therefore, the model for $\alpha_i$ can be a function of its own sharing ($l_i$) and the total information received from CYBEX. The following mathematical formula best captures the characteristics of $(\alpha_i)$ as described.

$$\alpha_i = \frac{\Gamma + l_i - \mathcal{F}(L_{-i})}{\mathcal{F}(L_{-i})}$$  \hspace{1cm} (6.3)

where, $\Gamma = \sum_{i \in N} \mathcal{L}_i$ is the maximum possible information exchanged in the sharing system by all the participating firms. $\mathcal{L}_i$ is the maximum amount of information that firm $i$ can share with other firms. $\mathcal{F}(L_{-i}) = \sum_{j \neq i} l_j$. $\mathcal{F}(L_{-i})$ represents the aggregate information received by firm $i$ and is assumed to be an increasing function of total information shared in the CYBEX framework. The detailed discussion of $\alpha_i$ is described later in subsection 6.2.2.
Chapter 6. Cyber-Investment and Cyber-Information Exchange Modeling

6.1.2.2 Cost Components Modeling

The information sharing activity costs a firm in several ways: (1) loss due to open access to protected assets, (2) reputation loss, (3) total investment, (4) participation cost, etc. Assuming the firm $i$ has proprietary asset of value $V_i$, the firm’s expected loss can be $p_i V_i$, where $p_i$ is the probability of occurrence of an attack event at that particular decision period. We model this probability as a function of a firm’s information sharing activity and the received information from CYBEX using dose-response immunity model, which is detailed later. The value of reputation loss for sharing $l_i$ amount of information is presented as $\zeta(l_i)$. The reputation loss function is assumed to be an increasing function, which signifies that the reputation loss of a firm varies in proportion to its sharing activity. We assume the CYBEX participation cost to be $c_p > 0$, thereby formulating the total cost component due to information sharing as $C_s = p_i V_i + \zeta(l_i) + I_i + c_p$. Now, combining the components together, the net payoff of firm $i$ playing with strategy $S_i$ can be expressed as:

$$U(S_i, S_{-i}) = a_0(\alpha_i l_i + \mathcal{F}(L_{-i})) \log(1 + I_i) - C_s$$  \hspace{1cm} (6.4)

6.1.3 Modeling $p_i$

The two major factors that influence probability of cyber attack on a firm are (1) degree of help from CYBEX ($\mathcal{F}(L_{-i})$), (2) amount of information the firm exchanges with CYBEX ($l_i$). $p_i$ is nothing but a risk evaluation parameter and the past researches in the field of medical sciences [100][101] have successfully used a method called dose-response model to quantify the hazard/risk posed by
an inoculated dose of organisms. This model has also been applied in wireless networks [102] to detect covert communication by attackers. In the context of cybersecurity information sharing, [103] mentions that dose-response function can be used as a tool for representing uncertain events and cyber attack is one of them. Even though modeling probability of cyber attack based on a firm’s sharing nature is always hard, the dose-response immunity (DRI) model can best capture the characteristics of cyber attack event according to our requirements. To appropriately model attack probability $p_i$, it must satisfy the following properties:

1. If a firm does not exchange any information, then its probability of getting attacked completely depends on the amount of information it receives for CYBEX and the security investment.

2. If every firm shares their information truthfully, then the total amount of information collected at CYBEX will be maximized and it could provide maximal benefit to each firm. As information sharing activity is maximal, the probability of cyber attack is expected to be diminished.

3. If CYBEX does not provide any help to the firms, due to the fact that no firm is interested to share, the probability of cyber attack completely depends on the security investment of the firms (as $l_i = 0$).

Let the ability of a drug to recover from a disease be $X_1$ and $X_2$ refers the immunity power of the patient in response to the drug. Assume an event $Y \in \{0, 1\}$ denotes the survival of patient, where value 0 refers to fully survived and 1 refers to death of the patient. If $p = \Pr\{Y = 1\} = 1 - \Pr\{Y = 0\}$, then
According to dose-response-immunity model,

\[
\text{logit}(p) = \ln \left( \frac{p}{1 - p} \right) = \beta^T X
\]  
(6.5)

where, \( X = [X_1, X_2]^T \) and \( \beta = [\beta_1, -\beta_2]^T \) represents the regression vector. The negative sign is to represent the inverse nature of dose and immunity.

In our model, the amount of CTI exchanged \((l_i)\) is analogous to dose of the drug and the received CTI from CYBEX is assumed to act as immune for the firm from cyber attacks. The event \(Y = 1\) refers to a failure to defend a cyber attack and \(Y = 0\) refers to successfully defend the cyber attack in our model. We assume that \( X = [\ln(1 + l_i), \ln(F(L_i))]^T \). We consider \( X_1 = \ln(1 + l_i) \) because the probability of cyber attack may not be zero if a firm does not share anything.

Using dose-response-immunity model given in Eqn. (6.5), the probability of a cyber attack can be expressed as:

\[
p_i = \frac{(1 + l_i)^{\beta_1}}{(1 + l_i)^{\beta_1} + (F(L_i))^{\beta_2}}
\]  
(6.6)

\(\beta_1\) represents the effectiveness of firm i’s shared information, and \(\beta_2\) refers to the effectiveness of others’ exchanged information in strengthening firm i’s security.

6.1.4 Modeling Reputation Cost \((\zeta(l_i))\)

The reputation cost \((\zeta(l_i))\) is assumed to be an increasing function in terms of total number CTI shared with CYBEX, i.e. \(\zeta'(l_i) > 0\). This emphasizes that the
loss in firms’ market value due to information exposure increases with increasing amount of shared CTI.

6.1.5 Optimization Problem

With the strategies and payoff model defined, the optimization problem for the firms in this game is to decide the optimal amount of information to share with CYBEX and the amount of security investment to make, so that the overall payoff will be maximized. Since the payoff function of a firm is guided by its own actions as well as the sharing action of other players too, deciding an optimal strategy $S_i$ for firm $i$ requires that the other players to play optimally too, so that social optimal equilibrium can be achieved. The optimization problem can be presented mathematically as the following:

$$\max_{I_i, l_i} U_i^{\text{net}}(S_i, S_{-i})$$

$$\max_{I_i, l_i} \left( \frac{(\Gamma + l_i - \mathcal{F}(L_{-i}))l_i}{\mathcal{F}(L_{-i})} + \mathcal{F}(L_{-i}) \right) a_0 \log(1 + I_i)$$

$$- \frac{(1 + l_i)^{\beta_1} V_i}{(1 + l_i)^{\beta_1} + (\mathcal{F}(L_{-i}))^{\beta_2}} - \zeta(l_i) - I_i - c_p$$

subject to the constraints

$$0 \leq I_i \leq B_i \quad \text{and} \quad 0 \leq l_i \leq L_i \quad \forall i \in \mathcal{N}$$

(6.8)
6.2 Game Analysis

In this section, we aim to analyze the above formulated non-cooperative game for extracting the possible equilibrium strategy profile when it is played simultaneously among the $N$ players. Considering a $N$-firm scenario, where each of them tries to maximize the optimization problem given in Eqn. (6.7), it can be seen that when $I_i > 0$, the firms’ discounted gain cannot be high if they free-ride on the received information from CYBEX. The framework ensures that when a firm abstains from sharing, the gain received from CYBEX decreases as free-riding is strongly discouraged in the system. Hence the greedy nature of a firm will never lead it to achieve a maximum reward. However, if it continuously increase the exchange of CTI, there is a chance it will receive higher reward than the previous greedy scenario. The sample numerical analysis given in Fig. 6.1 shows the declining nature (blue plot) of utility when the firm tries to free-ride by decreasing its breach sharing value from 35 to 0 starting at step 6. However, if it would have been shared truthfully, the payoff could have been more than the previous case as shown in the figure (red plot).

6.2.1 Existence of Nash Equilibrium

Here the net utility is analyzed to find a sufficient condition for the optimal security investment and information to share, such that the net payoff is maximized. This analysis will ensure the existence of socially-optimal equilibrium strategy for the firms, which will reward maximum provided every other firm plays with their best response strategies.
Lemma 6.1. *A firm will never share anything, when its budget for security investment is null, i.e. the dominant NE strategy of the game will be to not share any information.*

*Proof.* When a firm does not make any security investment, i.e. $I_i = 0$, then the gain component of net utility, as shown in Eqn. (6.7), is 0. Thus the net payoff is composed on only cost component, which will be maximized when the firm does not share anything ($l_i = 0$). Therefore, no sharing is the only Nash equilibrium in this scenario. Hence security investment is an important decision to make in the game, otherwise the framework will not be successful.

The following lemma proves the conditional existence of socially-optimal strategy profile that ensures the firms in maximizing their utility if they adhere to their corresponding optimal investment and amount of information to share.
Lemma 6.2. Socially-optimal strategy profile exists for the firm $i$ if every firm invests $I_i$ and truthfully share $l_i$ CTI with CYBEX, such that the following condition is satisfied.

$$p_i''V_iZ^2 + \zeta''(l_i)Z^2 - 2a_0Z\log(1 + I_i) - \frac{a_0(2a_i + l_i)^2}{(\alpha_i + Z)} > 0 \text{ where, } Z = F(L_{-i})$$

Proof. To prove the existence of socially-optimal strategy profile for the firm $i$’s multi-parameter net utility function, we need to show that there exists a tuple of security investment ($I_i$) and amount of information to share ($l_i$) which will maximize the net utility given in (6.7). Hence we must show that $U^\text{net}_i$ is strictly concave under the coupled constraint tuple ($I_i, l_i$). To prove it, we need to check whether the Hessian of $U^\text{net}_i$ is negative definite. Now differentiating Eqn. (6.7) with respect to $I_i$, we find

$$\frac{\partial U^\text{net}_i}{\partial I_i} = a_0(\alpha_i l_i + F(L_{-i}) - \frac{I_i}{1 + I_i} - 1$$

(6.9)

Similarly, differentiating $U^\text{net}_i$ with respect to $l_i$, we get

$$\frac{\partial U^\text{net}_i}{\partial l_i} = \frac{(\Gamma + 2l_i - F(L_{-i}))a_0 \log(1 + I_i)}{F(L_{-i})} - p_i'V_i - \zeta'(l_i)$$

(6.10)

where $p_i' = \frac{\beta_1(1 + l_i)(\alpha_i - 1)(F(L_{-i}))^{\beta_2}}{(1 + l_i)^\alpha + (F(L_{-i}))^{\beta_2}}$ is the first order differential of the attack probability with respect to $l_i$ and $\zeta'(l_i) > 0$ is assumed earlier.

The Hessian of $U^\text{net}_i$ can be represented as:

$$\mathcal{H} = \begin{bmatrix} \frac{\partial^2 U^\text{net}_i}{\partial l_i^2} & \frac{\partial^2 U^\text{net}_i}{\partial l_i \partial I_i} \\ \frac{\partial^2 U^\text{net}_i}{\partial I_i \partial l_i} & \frac{\partial^2 U^\text{net}_i}{\partial I_i^2} \end{bmatrix}$$

(6.11)
Chapter 6. Cyber-Investment and Cyber-Information Exchange Modeling

Again differentiating the first order differentials given in Eqn. (6.9) and (6.10) with respect to $I_i$ and $l_i$, then substituting in Eqn. (6.11), $\mathcal{H}$ can be re-written as,

$$\mathcal{H} = \begin{bmatrix}
-a_0(\alpha_i l_i + F(L_{i-1})) & a_0(\Gamma + 2l_i - F(L_{i-1})) \\
\frac{a_0(\Gamma + 2l_i - F(L_{i-1}))}{(1 + I_i)F(L_{i-1})} & \frac{2a_0 \log(1 + I_i)}{F(L_{i-1})} - p''_i V_i - \zeta''(l_i)
\end{bmatrix}$$

(6.12)

where, assuming $Z = F(L_{i-1})$, second order differential of $p_i$ can be defined as:

$$p''_i = \beta_1 Z^{\beta_2} (1 + l_i)^{\beta_1 - 2} \left[ (\beta_1 - 1) Z^{\beta_2} - (\beta_1 + 1)(1 + l_i)^{\beta_1} \right] / [(1 + l_i)^{\beta_1} + Z^{\beta_2}]^3$$

For $\mathcal{H}$ to be negative definite, the necessary and sufficient conditions are $\mathcal{H}_{11} = \frac{\partial^2 U_{net}^i}{\partial I_i^2} < 0$ and determinant of Hessian matrix must be positive, i.e. $\det(\mathcal{H}) > 0$.

As it is obvious from Eqn. (6.12), $\frac{\partial^2 U_{net}^i}{\partial I_i^2} = \frac{-a_0(\alpha_i l_i + Z)}{(1 + I_i)^2} < 0$, hence satisfies the first condition. Now, finding the determinant of $\mathcal{H}$:

$$\det(\mathcal{H}) = \frac{-a_0(\alpha_i l_i + Z)}{(1 + I_i)^2} \left[ \frac{2a_0 \log(1 + I_i)}{Z} - p''_i V_i - \zeta''(l_i) \right] - \frac{a_0^2(\Gamma + 2l_i - Z)^2}{(1 + I_i)^2 Z^2}$$

(6.13)

The determinant given in Eqn. (6.13) will be positive at the optimal $I^*_i$ and $l^*_i$, if the following condition is satisfied:

$$\frac{a_0(Z\alpha_i + l^*_i)^2}{(\alpha_i l^*_i + Z)} < p''_i V_i Z^2 + \zeta''(l^*_i) Z^2 - 2a_0 Z \log(1 + I^*_i)$$

$$\implies p''_i V_i Z^2 + \zeta''(l^*_i) Z^2 - 2a_0 Z \log(1 + I^*_i) - \frac{a_0(\alpha_i l^*_i + Z)}{(\alpha_i l^*_i + Z)} > 0$$

(6.14)

To find the optimal value of the coupled constraint parameters of the firm $i$ ($I^*_i, l^*_i$), we need to solve the first order differential equations given in Eqn. (6.9)
Chapter 6. Cyber-Investment and Cyber-Information Exchange Modeling

and (6.10) by equating them to zero. The optimal values can be found out by solving the following equations,

\[ I_i^* = a_0(\alpha_i l_i^* + Z) - 1 \]  
\[ p_i(l_i^*)V_i + \zeta(l_i^*) - \frac{(\Gamma + 2l_i - Z)}{Z}a_0 \log(1 + I_i^*) = 0 \]

This solution tuple constitutes the socially-optimal strategy of player \( i \). Hence the firms participating in the sharing framework will receive maximum utility if they play with their socially-optimal responses that follow the condition (6.14).

Given the condition (6.14) holds, it is clear that the Hessian \( \mathcal{H} \) of \( U_i^{net} \) is negative definite. Thus it proves the strict concavity nature of the utility function and the existence of socially-optimal equilibrium point for the coupled constraint optimization problem.

6.2.2 Guidance for CYBEX

As CYBEX coordinates the CTI exchange process among the participating corporations, its first and foremost goal is to self-motivate as many firms to participate in the sharing framework that will create a win-win situation for both the service-seeking firms as well as the CYBEX itself. Therefore, CYBEX requires a robust incentive model that will motivate the firms to share if they truthfully exchange their discoveries, whereas punish them if they try to free-ride on others’ shared information. The robust incentive model \( (\alpha_i) \) for CYBEX can suitably reward/punish the firms depending on how they are contributing to the sharing framework. If a firm shares more information whereas other participating firms are not, then CYBEX rewards the former firm more to keep it motivated towards
sharing. However, if it shares minimum and the rest of the firms have exchanged a large amount of information, then this is a case of free-riding of the former firm. In this situation, CYBEX rather punishes with low \( \alpha_i \) value to prevent such information exploitation scenarios. The reward of sharing effectiveness value \( (\alpha_i) \) is comparatively high when the overall system of participants are at the initial stages and need to be motivated to share more, whereas when the sharing system is stable and every firm is willing to share its security information truthfully, \( \alpha_i \) can decrease to a lower value to let the sharing framework self-sustain. Based on the above characteristics, the following incentive model best fits for CYBEX’s requirements and can be represented as:

\[
\alpha_i = \Gamma + l_i - \frac{\mathcal{F}(L-i)}{\mathcal{F}(L-i)}.
\]

The following insights can be deduced to understand the physical significance of the above equation. When, the sharing amount \( (l_i) \) of firm \( i \) increases and other participants do not share a lot i.e. \( \mathcal{F}(L-i) \) is low then the reward \( \alpha_i \) provided by CYBEX is high, thus motivating the firm \( i \) to continue its sharing. However, when \( l_i \) is low, and \( \mathcal{F}(L-i) \) is high, then firm \( i \) is trying to free-ride, and CYBEX rewards low \( \alpha_i \) value to prevent such behavior.

### 6.3 Results and Discussion

Here, we present the results obtained from numerical analysis and simulations to validate our cybersecurity information sharing model. To show the existence of socially-optimal equilibrium security investment and information sharing strategies of a firm, we used the net utility expression given in Eqn. (6.7). The regression parameters in the attack probability model are considered as: \( \beta_1 = 5, \beta_2 = 3 \). The reputation function, \( \zeta(l_i) \) is considered to be a quadratic expression
equivalent to \( w_1 l_i \), where \( w_1 > 0 \). The received information set \( F(L_{-i}) \) from CYBEX is assumed to be the total amount of information exchanged by other participating firms except \( i \), thus \( F(L_{-i}) = \sum_{j \neq i} l_j \). For the experiment, we assume that each firm has total 25 information to share \( (L) \) and has total budget \( (B) \) of 350 to invest.

To prove the consistency of condition (6.14), we first find the feasible \( l_i \) and the corresponding \( F(L_{-i}) \) numerically using Eqn. (6.16). Considering a single tuple \( (I_i^*, l_i^*, F(L_{-i})) \) that satisfies the condition (6.14), we tested whether this tuple is in fact the socially-optimal (SO) tuple by experimenting with different \( I_i \) and \( l_i \) values other than \( I_i^*, l_i^* \) respectively. In Fig. 6.2(a), we find that \( I_i^* = 181.1 \) value is the SO-strategy because (1) it satisfies the condition (6.14), (2) deviating from this investment and taking random investments below/above this value could not reward more. For this experiment, we keep the \( l_i^*, F(L_{-i}) \) values fixed. Then we performed a similar experiment to verify, whether the optimal information sharing value \( (l_i^* = 14.25) \) is also a SO-strategy or not by keeping \( I_i^*, F(L_{-i}) \) values fixed. It is found from Fig. 6.2(b) that \( l_i^* \) that follows
the condition (6.14), returns highest utility which cannot be achieved by other different $l_i$ values. Therefore, it can be ensured that if the tuple $(I_i^*, l_i^*, F(L_{-i}))$ satisfies condition (6.14), then it is a socially-optimal equilibrium strategy profile for firm $i$.

In order to understand the nature of investment of a firm $i$, where other participating firms share a fixed amount of information, we present a sample scenario in Fig. 6.3. It is noticed that there exists an optimal amount of information to be shared ($l_i$) at which the net utility is maximized for a particular investment quantity. It is also observed that the optimal sharing amount increases as the firms make higher security investment to discover more information. However, it is not true that a firm will receive larger payoff upon large investment, rather the cost component dominates over outcome of such huge investment after a certain threshold. From the plot, we see that the firm receives increasing reward when $I_i$ is increased from 100 to 400. However, further increase in the
investment amount does not increase the net utility any more. Thus it can be inferred that there exists an optimal peak investment limit beyond which the firms cannot gain high benefit. However, the optimal investment amount might vary depending on total number of security information received from CYBEX in that decision period.

![Net utility variation at simultaneous optimization of Investment ($I_i$) and amount of information shared ($l_i$)](image)

**Figure 6.4:** Net utility variation at simultaneous optimization of Investment ($I_i$) and amount of information shared ($l_i$)

In Fig. 6.4, the firm’s investment and information sharing amount are varied simultaneously to verify the nature of net utility function. Assuming a total 50 units of vulnerability information shared by the other participating firms, it is found that the net payoff for firm $i$ can be maximized for a particular strategy tuple ($I^*_i$, $l^*_i$), when it satisfies the condition given in Eqn. (6.14). This strategy profile lies in between the white circle on top of the curve presented in the Fig. 6.4 that corresponds to the maxima of the utility function. This proves the existence
of the socially-optimal decision parameters for the current scenario that satisfy the derived condition in Section 6.2.

6.4 Summary

In this Chapter, we studied a simultaneous non-cooperative game where, firms aim to decide the optimal amount of cyber-investment and cyber-information exchange simultaneously. We modeled a novel payoff function for the firms by incorporating the risk of cyber attacks for threat information exchange. We borrowed an inter-disciplinary model from biology called dose-response immunity model to formulate the probability of cyber attack. Finally, we proved the existence of Nash equilibrium strategy for the coupled constraint optimization problem using negative definite Hessian condition and derive the optimal value of tuple (cyber-investment amount, cyber-information sharing amount) that maximize the firms’ net payoff.
Chapter 7

Cyber-Threat Information Sharing in Cloud Platform

Cloud computing is one of the fastest growing segments of the cyberspace. That is because cloud computing is cost efficient, e.g., cloud users can reduce spending on technology infrastructure and have easy access to their information without up-front or long-term commitment of resources. However, security in cloud computing is more challenging than the security of traditional networks. That is because Virtual Machines (VMs) can start, stop, and move from hypervisor to hypervisor at the click of a button. Cloud security techniques have to be able to easily deal with these movements. Therefore, a game theoretic model for traditional network may not be suitable in a cloud computing environment. Moreover, different public cloud users share a common platform such as the hypervisor. A common platform intensifies the well-known problem of cybersecurity interdependency [104–107] as an attacker who gains access to the hypervisor can start, stop, and modify all of the VMs that are housed on that
Chapter 7. *Cyber- Threat Information Sharing in Cloud Platform*

hypervisor. The result is a more challenging execution environment due to the risk aggregation from many users sharing the same platform. A single attack on a cloud provider can compromise thousands of users at a huge cost.

This chapter considers a set of users in a public cloud who share the same hypervisor. The goal of our game model is to provide incentive to all cloud participants to invest in vulnerability discovery and share their cyber-threat information despite the potential cost involved. In particular, our game model will find out what are the necessary conditions under which a rational user in a public cloud will share his discovered vulnerabilities.

### 7.1 System Model

The system model considered here is extended from [60], where $m$ different users operate over a public cloud environment. Each user $i \in \{1, 2, \cdots , m\}$ may have $k$ multiple applications running on the cloud operating system as shown in Fig. 7.1 and the monitor application is one of them. We consider that the monitor application can perform following tasks: (1) collects cyber-threat information by monitoring the activities on VMs, (2) actively shares the threat knowledge with other VMs and Information Sharing and Analysis Center (ISAC), (3) gathers information shared by other entities and apply to enhance security of user VMs as well as operating systems.

In our architecture, we consider that multiple VMs share a common hardware and hypervisor such as Kernel-based Virtual Machine (KVM), Xen, and VMware. Thus, the applications running on the operating systems have access to the common hardware, which is why any vulnerability found in applications of one
user may cause a collateral damage to other users provided the attacker can successfully compromise the hypervisor. In our model, we neglect the possibility of random hardware failure of cloud system, but focus on the intelligent cyber-attacks. Since the user VMs are sharing a common platform, one’s security is interdependent on others. So it is necessary for the providers to constantly monitor and share the threat information with users. Otherwise, attackers may compromise user VMs and then possibly exploit the common hypervisor using the compromised VMs. Considering the propagation of attacks and their consequences, we categorize attacks to: (1) restricted attacks, and (2) unrestricted attacks. In case of restricted attacks, the malicious agent could only compromise the user VM but not the hypervisor, whereas unrestricted attacks could exploit both user VM and hypervisor which may potentially affect other co-residing user VMs on the same hypervisor. For preventing the possibility of collateral damages, rational users should share their threat related discoveries with each other. We model the following game to analyze, whether a cloud user would prefer to make security investment and share its threat knowledge or not, given probabilistic nature of attack success.

### 7.2 Game Model

Cyber-threat information sharing in a public cloud is a scenario suitable for game theoretic analysis. That is because common resources shared by users such as the hypervisor make the security of each user directly dependent on the security of others and these externalities are often overlooked.
We consider a two player game with two users that can share their vulnerabilities through the Information Sharing and Analysis Center, as in Fig. 7.1. The players are User $i$ and User $j$ that share the same hypervisor on a public cloud as also illustrated in Fig. 7.1. The exact number of vulnerabilities $N$ in the public cloud is unknown but has an expected value $n$ known to the two players. Fig. 7.2 shows the Venn Diagram illustration of discovered vulnerabilities when both users invest to discover those vulnerabilities. A user that does not invest to discover vulnerabilities will not discover any vulnerability and thus has nothing to share. A user that invests in the discovery of vulnerabilities will not discover all the vulnerabilities, so it is realistic to assume that some of the vulnerabilities may go
undetected despite the users’ investment. Users’ investment in our model is not to gather and examine the information about past cyber-attacks (e.g., forensic), but to discover the vulnerabilities and patch the system (VMs) before an attacker can exploit those vulnerabilities to launch an attack. Users invest as a proactive measure. However, any model that deals with vulnerabilities post-attack could also be superposed to this model.

In the Venn diagram of Fig. 7.2, the set of vulnerabilities discovered by User $i$, User $j$, and the attacker are represented by $V_i$, $V_j$ and $V_a$ respectively. Recall that a user who does not invest to discover vulnerabilities will not discover any vulnerability. Therefore, $V_i$ (respectively $V_j$) is an empty set if User $i$, (respectively User $j$) choose not to invest. However, the set $V_a$ is never empty since by its nature, the attacker is always looking for new vulnerabilities. $V_{aij}$ represents the set of undiscovered vulnerabilities. The probability that a vulnerability belong to


<table>
<thead>
<tr>
<th>Parameters</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>$c$</td>
<td>Cost of investment in vulnerability discovery</td>
</tr>
<tr>
<td>$d$</td>
<td>Damage caused by an exploited vulnerability</td>
</tr>
<tr>
<td>$s$</td>
<td>Expected cost of sharing a vulnerability</td>
</tr>
<tr>
<td>$N$</td>
<td>Number of vulnerabilities</td>
</tr>
<tr>
<td>$n$</td>
<td>Expected number of vulnerabilities</td>
</tr>
<tr>
<td>$P_i, P_j = p$</td>
<td>Probability that User $i$ / User $j$ discovers a vulnerability given that he has invested</td>
</tr>
<tr>
<td>$P_a = p$</td>
<td>Probability that the attacker discovers a vulnerability</td>
</tr>
<tr>
<td>$\pi$</td>
<td>Probability that the attacker compromises the hypervisor given that a VM is compromised</td>
</tr>
</tbody>
</table>

| Table 7.1: Notations |

The set $V_i, V_j$ or $V_a$ is given by $P_i, P_j$ and $P_a$ respectively. Those probabilities can be estimated using a red team experiment in a cloud to find the average number of vulnerabilities a player discovers. Remember that $P_i = 0$ (respectively $P_j = 0$) if User $i$, (respectively User $j$) choose not to invest. Similarly, the definition of $P_{ij}, P_{ai}, P_{aj}, P_{aij}$, and $P_{aij}$ follow from the Venn diagram of Fig. 7.2.

We assume that the attacker and the two users have similar capabilities to discover vulnerabilities and they independently discover those vulnerabilities.

\[
P_i = P_j = P_a = p 
\]

\[
P_{ij} = P_{ai} = P_{aj} = p^2 
\]

\[
P_{aij} = p^3 
\]

However, it is straightforward to extend our model to the case that the attacker and the two users have different capabilities to discover vulnerabilities and their discovery of a vulnerability is not independent.

We denote by $c$ a user’s cost associated with the investment in vulnerability discovery. We assume that both users have similar costs and that the vulnerabilities
are homogeneous. Moreover, we consider that the attacker is always successful when exploiting a vulnerability that is not discovered or shared between users. When a vulnerability is not discovered by User $i$ and User $j$ also does not discover it or decides not to share that vulnerability with User $i$, then an attacker can exploit that vulnerability and this will result in a damage to User $i$ that we denote $d$, and vice versa.

When User $i$ discovers a vulnerability and decides not to share it with User $j$, then the same vulnerability can be exploited by the attacker to launch an attack on User $j$ (in case User $j$ has not discovered that vulnerability), compromise the hypervisor with probability $\pi$ and then compromise User $i$ through a side channel attack. Thus, the possibility of side channel attack can constrain User $i$ to share its discovered vulnerability. There is a cost $s$ involved when a user shares a vulnerability. This represents the potential reputation lost, liability, and risk of lawsuit. Our stage game in normal form is represented in Table 7.2, which is a symmetric game. Each user decides to invest in vulnerability discovery and to share those vulnerabilities simultaneously in a one-shot game. Thus, the three strategies available to a user are: not invest and not share ($\bar{I}\bar{S}$); invest and not share ($IS$); and invest and share ($I\bar{S}$). The strategy not invest and share ($I\bar{S}$) is not a possibility because a user that does not invest will not discover any vulnerability and cannot have any vulnerability to share.

The payoffs in Table 7.2 are calculated according to Equation (1), (2), (3), the Venn diagram in Fig. 7.2, and the parameters in Table 7.1. For instance, in the strategy profile ($I\bar{S},\bar{I}\bar{S}$), the payoff for User $i$ has two components. A loss from direct attack is the product $pmd$ because the attacker discovers a vulnerability with probability $p$, the expected number of vulnerabilities is $n$, and each vulnerability
\[ \begin{array}{ccc}
\text{USER } i & \text{User } j & \text{USER } j \\
\bar{I} & \{ -pnd - \pi pnd; \\
& -pnd - \pi pnd \} & \bar{I} & \{ -pnd - \pi (p - p^2)nd; \\
& -c - (p - p^2)nd - \pi pnd \} & \bar{I} & \{ -(p - p^2)nd - \pi (p - p^2)nd; \\
& -c - spn - (p - p^2)nd - \pi (p - p^2)nd \} \\
\bar{I} & \{ -c - (p - p^2)nd - \pi pnd; \\
& -pnd - \pi (p - p^2)nd \} & \bar{I} & \{ -c - (p - p^2)nd - \pi (p - p^2)nd; \\
& -c - (p - p^2)nd - \pi (p - p^2)nd \} & \bar{I} & \{ -(p - p^2)nd - \pi (p - p^2)nd; \\
& -c - spn - (p - p^2)nd - \pi (p - p^2)nd \} \\
I & \{ -c - spn - (p - p^2)nd \\
& -\pi(p - 2p^2 + p^3)nd; \\
& -c - (p - 2p^2 + p^3)nd \} & I & \{ -c - spn - (p - 2p^2 + p^3)nd \\
& -\pi(p - 2p^2 + p^3)nd; \\
& -c - spn - (p - 2p^2 + p^3)nd \} \\
I & \{ -(p - p^2)nd - \pi (p - p^2)nd \} & I & \{ -(p - p^2)nd - \pi (p - p^2)nd \} \\
& -\pi(p - p^2)nd \\
& -c - (p - 2p^2 + p^3)nd \\
& -\pi(p - 2p^2 + p^3)nd \}
\end{array} \]

**Table 7.2:** Game in Normal Form
causes damage $d$. A loss from side channel attack is the product $\pi pnd$ because a side channel attack goes through User $j$ (thus the product $pnd$ as explained above) and the hypervisor gets compromised with probability $\pi$. Furthermore, we add the cost $c$ when a user invests and the cost $spn$ when a user shares. The different probabilities are adjusted depending on the action chosen by a user and its opponent.

As another example, the payoff for User $i$ for the strategy profile $(I\bar{S}; I\bar{S})$ is $-c - (p - p^2)nd - \pi(p - p^2)nd$, which has three components. The first component is $-c$, the cost of investment. The second component is $-(p - p^2)nd$, the loss from direct attack with probability $p(1 - p)$ or $(p - p^2)$. Recall that an attack is successful when the attacker discovers a vulnerability (with probability $p$) but the firm does not discover it (with probability $(1 - p)$). Multiplying both yields $p(1 - p)$. The third component is $-\pi(p - p^2)nd$, the loss from side channel attack.

### 7.3 Game Analysis

The game in Table 7.2 is a symmetric game. We analyze the game and present the possible Nash Equilibrium (NE) profile.

**Lemma 7.1.** The game has pure strategy Nash equilibrium $(I\bar{S}; I\bar{S})$, if the following two conditions are satisfied: (i) $c > p^2nd$, and (ii) $c + spn > (1 + \pi)p^2nd$.

**Proof:** The symmetric game presented in Table 7.2 has pure NE strategy $(I\bar{S}; I\bar{S})$, if strategy $I\bar{S}$ is the best response strategy of user $i$ as well as user $j$. Therefore, user $i$ and $j$’s best strategy must be $I\bar{S}$. Hence there is no profitable deviation from strategy $(I\bar{S}; I\bar{S})$. As the game is symmetric in nature, it is sufficient to
check the best response conditions of one player, which will also be same for
the other player too. This assumption has been considered for proving the
other lemmas presented later in the chapter. Now we can derive the following
conditions through best-response analysis.

\[-p_{nd} - \pi_{pnd} > -c - (p - p^2)nd - \pi_{pnd}\]
\[\implies c > p^2 nd \] (7.4)

\[-p_{nd} - \pi_{pnd} > -c - spn - (p - p^2)nd - \pi(p - p^2)nd\]
\[\implies c + spn > (1 + \pi)p^2 nd \] (7.5)

Lemma 7.2. The game has pure strategy Nash equilibrium \((I \bar{S}; I \bar{S})\), if the following
two conditions are satisfied: (i) \(c < p^2 nd\), and (ii) \(s > \pi pd\).

Proof: Both users prefer to invest in vulnerability discovery but do not share
their discoveries, if there is no profitable deviation from the strategy \((I \bar{S}; I \bar{S})\).
We now obtain the necessary conditions.

\[-p_{nd} - \pi(p - p^2)nd < -c - (p - p^2)nd - \pi(p - p^2)nd\]
\[\implies c < p^2 nd \] (7.6)

And,
\[-c - spn - (p - p^2)nd - \pi(p - 2p^2 + p^3)nd\]
\[< -c - (p - p^2)nd - \pi(p - p^2)nd\]
\[\implies s > \pi dp(1 - p) \] (7.7)

Lemma 7.3. The game has pure strategy Nash equilibrium \((I S; I S)\), if the following
two conditions are satisfied: (i) \(c + spn < (1 + \pi)ndp^2(1 - p)\), and (ii) \(s < \pi dp(1 - p)\).
Proof: Both users invest in vulnerability discovery, and prefer to share the discovered vulnerability if there is no profitable deviation from the strategy profile \((IS; IS)\). Thus, \((IS; IS)\) will be NE strategy profile, provided the following conditions are satisfied.

\[-(p - p^2)nd - \pi(p - p^2)nd < \]
\[-c - spn - (p - 2p^2 + p^3)nd - \pi(p - 2p^2 + p^3)nd\]
\[\Rightarrow c + spn < (1 + \pi)ndp^2(1 - p) \quad (7.8)\]

And,
\[-c - (p - 2p^2 + p^3)nd - \pi(p - p^2)nd\]
\[< -c - spn - (p - 2p^2 + p^3)nd - \pi(p - 2p^2 + p^3)nd\]
\[\Rightarrow s < \pi dp(1 - p) \quad (7.9)\]

Lemma 7.4 (a). If Equation (7.4) and (7.5) hold true, then \((\bar{I}S; \bar{I}S)\) is the only Nash equilibrium of the game.

(b). If Equation (7.6) and (7.7) hold true, then \((I\bar{S}; I\bar{S})\), is the only Nash equilibrium of the game provided one of the following conditions hold true. (i) \(c > \pi pd\), or (ii) \(c + spn > (1 + \pi)p^2 nd\)

(c). If Equation (7.8) and (7.9) hold true, then \((IS; IS)\) is the only Nash equilibrium of the game.

Proof 7.4 (a): As shown in Equation (7.4) and (7.5), strategy \(\bar{I}S\) is best response strategy of user \(i\) and user \(j\) due to the symmetric nature of the game. Thus \((\bar{I}S; \bar{I}S)\) is a NE strategy profile. It can be observed that the strategy profile \((I\bar{S}; I\bar{S})\) cannot be a NE as the conditions (7.4) and (7.6) act opposite to each other. Similarly, \((IS; IS)\) is also not NE because of the conflicting nature of
Chapter 7. Cyber-Threat Information Sharing in Cloud Platform

conditions (7.5) and (7.8). Now the NE profiles \((IS; IS)\) and \((I\bar{S}; IS)\) are possible if (i) \(s < \pi dp(1 - p)\) and (ii) \(c + spn < (1 + \pi p)^2 nd - \pi p^3 nd\) hold true. However, the condition (ii) cannot be true because Equation (7.5) states the opposite. Hence \(IS\) cannot be a best response strategy of user \(i\), when user \(j\) plays strategy \(I\bar{S}\) and vice-versa. Therefore, \((I\bar{S}; I\bar{S})\) is the only NE of the game when equation (7.4) and (7.5) hold true.

Proof 7.4 (b): From Equation (7.6) and (7.7), we can state that \(I\bar{S}\) is best response strategy of user \(i\) as well as user \(j\). Thus, it is a NE strategy profile. Due to symmetric nature of the game, it is true that no other row/column strategy that intersects cell \((I\bar{S}; I\bar{S})\) can be NE too. The strategy profiles \((I\bar{S}; I\bar{S})\) and \((IS; IS)\) also cannot be NE because relational constraints (7.6) and (7.7) are not valid for the corresponding NE conditions given in Equation (7.4) and (7.9) respectively. However, the strategy profiles \((IS; I\bar{S})\) and \((I\bar{S}; IS)\) can be NE, provided the following conditions are satisfied:

\[-pnd - \pi pnd < -c - spn - (p - p^2)nd - \pi(p - p^2)nd\]
\[\implies c + spn < (1 + p)p^2 nd \quad (7.10)\]

And,
\[-c - (p - p^2)nd - \pi pnd\]
\[< -c - spn - (p - p^2)nd - \pi(p - p^2)nd\]
\[\implies s < \pi pd \quad (7.11)\]

However, this equilibrium strategy must be avoided to derive conditions for unique Nash equilibrium strategy. Therefore, the strategy profile \((I\bar{S}; I\bar{S})\) can be the unique NE in this scenario, only when either condition (7.10) or (7.11) does not hold true.
Proof 7.4 (c): This lemma can be proved in the similar manner as the lemma 7.4(a) proved earlier. It can be observed that the condition (7.8) and (7.9) ensure that IS is the best response strategy of both players. This voids the chances of other possible NE strategies such as (I ̄S; ̄I S) and (I S; ̄I S) because the relational constraints (7.8) and (7.9) do not hold true for their NE conditions given in Eq. (7.5) and (7.7). Thus, it is mandatory to show that the strategy profiles (I ̄S; I S) and (I S; ̄I S) are not the NE strategies. These two strategies can be NE only when the conditions (i) \( s > \pi pd \) and (ii) \( c < p^2 nd \) are satisfied. However, the condition (ii) cannot be true as the condition \( s < \pi pd(1 - p) \) should be true as per Equation (7.9) to let the strategy profile (IS; IS) be the Nash equilibrium strategy. Hence, the strategy profile (IS; IS) is the unique NE profile in this situation provided the condition (7.8) and (7.9) are satisfied.

7.4 Numerical Results and Discussion

In this section, we report the results obtained from numerical analysis, showing the regional Nash equilibrium plots under different values of the critical parameters like vulnerability discovery probability (p), damage caused due to exploiting the discovered vulnerability (d), probability that attacker compromises the hypervisor (\( \pi \)), cost of investment (c), and cost of sharing a vulnerability (s).

Fig. 7.3 depicts the possible Nash equilibrium strategy profiles when the damage caused by a vulnerability and probability of attacker compromising hypervisor vary, assuming \( c = 1 \), \( n = 10 \), \( s = 0.3 \), and \( \pi = 0.1 \). We observe that users prefer to both invest for vulnerability discovery and share them when the damage caused due to the vulnerability and probability that an attacker compromises
the hypervisor is high. So the investment towards vulnerability discovery and sharing with peers help the users to prevent the attacker’s effort to find the same vulnerability and exploit it. However, when the damage cost is low and probability of compromising the hypervisor is also low, then the users better off not sharing their discoveries because they do not lose substantially than when sharing their vulnerabilities. The crucial point to notice here is that the users must invest to discover vulnerabilities regardless of the damage caused by exploiting the vulnerability and the probability of an attacker compromising the hypervisor, which will benefit the users to remain secured from the attacker’s exploitation using the undiscovered vulnerabilities. However, sharing is a choice for the users dependent on the cost involved in it. To understand the NE strategy profile when vulnerability discovery probability \( p \) and hypervisor compromising probability \( \pi \) vary, we have conducted experiment to find the Nash equilibrium strategies for different \( \pi \) and \( p \) values by fixing the value of damage \( d \) as 20 and keeping
the value of other variables intact. As shown in Fig. 7.4, the users prefer to invest in vulnerability discovery and share, if the discovering probability is not very low or very high and hypervisor compromising probability is not very low. This case occurs due to benefits of investment and sharing, which cannot be derived from strategies \((\bar{I} S; \bar{I} \bar{S})\) or \((I \bar{S}; I \bar{S})\). However, at very low probability of vulnerability discovery \(p\), all players are demotivated to invest. When \(p\) increases and \(\pi\) is low, the users prefer to invest without sharing their discoveries because the attacker is less likely to compromise the hypervisor. At very high probability of vulnerability discovery \(p\), sharing vulnerability is not profitable because each player has a high chance to discover all vulnerability itself without relying on the help of others.

In Fig. 7.5, we analyze the NE strategy profiles at different regions of \(p\) and \(d\)
Chapter 7. Cyber-Threat Information Sharing in Cloud Platform

**Figure 7.5:** Probability that attacker compromises hypervisor vs. Damage caused

**Figure 7.6:** Cost of sharing vs. Cost of Investment
combinations. Interestingly, we find that users are more inclined to invest in vulnerability discovery after a certain threshold of discovering probability \( (p) \) beyond which users are satisfied with their vulnerability discovery. However, they do not share these discoveries until damage cost exceeds a limit, after which the users better off taking the NE strategy \((IS; IS)\). It can be understood that users do not invest or share if the discovery probability is very low, as the difficulty in discovering any vulnerabilities prohibit investment. Hence, very high investment might not help in improving the vulnerability discovery process. There remains a small chance that a user might free-ride on another user’s vulnerability discovery if they can easily discover the vulnerabilities, i.e. the probability of vulnerability discovery is close to 1. Therefore, this kind of scenario must be avoided to ensure that every player truthfully behaves and reciprocates the exchange of vulnerability discoveries.

Fig. 7.6 gives a summary of NE profiles at different cost of investment \((c)\) and sharing vulnerability \((s)\) assuming \(d = 20, p = 0.6\), while keeping other parameter intact. The users are inclined to invest for vulnerability discovery and share them only when the cost of investment and sharing is low. If the cost of investment is very high then the users avoid investment, thus do not share as well. It is observed that if the cost of investment is less than certain threshold value and expected cost of vulnerability sharing is more than certain limit, the users prefer not to share any vulnerabilities even though they invest to discover more vulnerabilities. The center region and black region in the plot are the special cases where, one user might take strategy IS and other takes exactly opposite, resulting in a free-ride situation on the former user’s shared information. Free-riding behavior can be prevented by choosing the cost of investment and cost of sharing carefully, which ensures that the players do not fall into the center
or black region. Finally, we plot the expected payoff variation with respect to increasing vulnerability discovery probability \((p)\) and damage cost \((d)\) in Fig. 7.7. The dark bars in the figure point that the user changes his strategy after the occurrence of the bar. The net payoff function follows a downward concave characteristics w.r.t. probability of discovering vulnerability. We observe that when the damage cost is low \((d = 5)\), then the user mostly sticks to the NE strategy \((I\bar{S}; I\bar{S})\) after the vulnerability discovery probability \((p)\) exceeds 0.15, which is the center region of curve representing \(d = 5\). However, when \(p\) is very low the users neither invest nor share. As shown in the plot, interesting scenarios occur when the damage cost \((d)\) increases. The users choose \((I\bar{S}; I\bar{S})\) when \(p\) is close to 0, but they change their strategy to \((I\bar{S}; I\bar{S})\) quickly depending on how large is the damage \((d)\). In the plot, the payoff jumps to a relatively higher value, when the users update their strategy \((I\bar{S}; I\bar{S})\) to \((IS; IS)\) and degrades to
a lower value when they do the vice-versa. This strategy reversal happens when
the probability of discovering vulnerability \((p)\) is very high, where the users feel
confident about discovering breaches on their own and do not want to share any
of their discoveries with other user. As the damage \((d)\) increases to very high
value, the users mostly prefer to invest and share, whereas the payoff received is
minimal.

7.5 Summary

In this Chapter, we extended the notion of cyber-threat information sharing
to cloud computing domain. Since multiple virtual systems share a common
platform called hypervisor, it is important for the residing systems to collaborate
with each other by sharing vulnerability information among themselves so that
malicious intruder has less chance to compromise them directly or through side-
channels. We, therefore, formulated a non-cooperative game among public cloud
users where the players are incentivized to invest in vulnerability discovery and
share with other users in presence of potential cost of sharing. Using best-
response analysis, we presented the possible Nash equilibrium (NE) solutions
out of “no investment and no share”, “invest and no share”, “invest and share”
strategies and conditions under which the NE(s) can be achieved.
Chapter 8

Conclusions and Future Work

In this research, we investigate the issues of cybersecurity information sharing among various corporations to support them in building a nation-wide robust security infrastructure that will provide proactive defense ability from the cyberwars. We have conducted a detailed literature survey on the prior research works in this domain and present the concise summary. Many efforts to design policies, frameworks, standards, models from government, industries, academia to enable cyber-threat intelligence sharing motivate our work presented in this dissertation. Understanding both pros and cons of cyber-information sharing, we pose various constraints that might create roadblocks in bringing a successful cyber-threat information sharing framework.

First, we formulate an evolutionary game model to understand how competing firms in a non-cooperative game can decide independently whether to participate in the CYBEX and share or not. We use evolutionary dynamics to analyze both participation and information sharing game and understand the outcomes of the game, i.e. evolutionary stable strategies (ESS). Various conditional constraints
Chapter 8. Conclusions and Future Work

derived from the analysis have helped to devise a dynamic cost adaptation algorithm that exploits the participation cost to act like an incentive in the beginning so as to motivate as many firms to participate. However, as the participation strength grows, the incentive gradually turns to be a cost and let the sharing system to self-sustain, leading to a win-win situation. We also propose a distributed learning heuristic for the participating firms to let them attain ESS by learning from the history information. Secondly, we extend the CYBEX participation game to model a 3-strategy information sharing game, where the firms potentially figure out how much of their CTI they want to share with the community of firms. Using evolutionary analysis, we analyze the constraints under which different equilibrium strategies can be achieved and then show that various external incentives from CYBEX can be opted in an appropriate manner to motivate firms towards sharing all of their information truthfully, thus avoiding free-riding in the system.

Then, we devise a non-cooperative game between $N$ firms, who participate in CYBEX, aims to find how much a firm would want to invest and share under the distributed competitive sharing environment. We model this as an optimization problem by formulating a utility function for the firms and solved to find the socially-optimal equilibrium point, consisting of the tuple (amount of investment and quantity of information to share) that maximizes the firms’ net reward. We present the numerical results to verify the existence of the socially-optimal strategy profile and proposed guidance for CYBEX to motivate the firms towards actively participate and share in the framework. Lastly, we have proposed an analytical framework that uses game theory to model cyber-threat information in public cloud computing. The game theoretic model captures the trade-offs between the desirable security of public cloud users and the risk of sharing.
cyber-threats. Our game theoretic framework captures the conditions under which public cloud users are motivated to monitor and to share cyber-threats. At very low probability of vulnerability discovery, all players are demotivated to invest and then will not share any vulnerability. Also, user will not share vulnerability if they are easy to discover.

8.1 Future Work

In the future, we plan to extend our research by addressing the following important problems:

- Considering an APT attack model, where the users may not detect the attacks immediately after the attack incurred rather detect after certain stages passed, we plan to model a sequential game between an attacker and a pair of firms. The firms in the game would prefer to act sequentially; first with investment strategy and then with sharing strategy, where that attacker’s strategy would be to perform tactful attack on one of the firms in a cloud environment. Thus a zero-sum utility can be used to model the payoff for the attacker as well as the firms. The cost function for the firms must be a function of its investment and sharing, but it also depends on the attack probability of attacker. We plan to derive inferences on firms’ optimal strategies that would lead to win the game of defense and understand under what scenarios rational attacker will abstain to attack the system.
• The corporations belong to different sectors according to their nature of business operations and they might have different services/applications for running their businesses. Intensity of cyber-criminal activities mostly depend on the sectors a firm belongs to. So it will be crucial to investigate whether similar sector firms would like to form coalition among each other to exchange cybersecurity information or they better stay isolated to maintain competitive advantage. So we plan to formulate a coalitional game model to analyze whether firms would prefer to form coalitions and share their threat data inside the community, or not.
Bibliography


