

# **AN EXPERIMENTAL AND COGNITIVE APPROACH TO CYBERSECURITY FOR BUILDING A SECURE CYBERSPACE**

*a Thesis submitted by*

Zahid Maqbool

(D14038)

*for the award of the degree of Doctor of Philosophy*



**SCHOOL OF COMPUTING & ELECTRICAL ENGINEERING**

**INDIAN INSTITUTE OF TECHNOLOGY MANDI**

December 8, 2020



## THESIS CERTIFICATE

This is to certify that the work contained in the thesis entitled “A game-theoretic and cognitive approach to cybersecurity for building a secure cyberspace.” being submitted by Mr. Zahid Maqbool (Enroll. No: D14038) has been carried out under my supervision. In my opinion, the thesis has reached the standard fulfilling the requirement of regulation of the Ph.D. degree. The results embodied in this thesis have not been submitted elsewhere for the award of any degree or diploma.

December 8, 2020


Dr. Varun Dutt (Supervisor)  
Associate Professor  
School of Computing and Electrical Engineering  
School of Humanities and Social Sciences  
Indian Institute of Technology Mandi  
Kamand, Himachal Pradesh, India  
Email: [varun@iitmandi.ac.in](mailto:varun@iitmandi.ac.in)

### Declaration by the Research Scholar

I hereby declare that the entire work embodied in this Thesis is the result of investigations carried out by me in the *School of Computing and Electrical Engineering*, Indian Institute of Technology Mandi, under the supervision of *Dr. Varun Dutt*, and that it has not been submitted elsewhere for any degree or diploma. In keeping with the general practice, due acknowledgments have been made wherever the work described is based on findings of other investigators.

Place: IIT Mandi, Kamand

Date: December 8, 2020

Signature: 

Name: Zahid Maqbool

### Declaration by the Research Advisor

I hereby certify that the entire work in this Thesis has been carried out by *Zahid Maqbool*, under my supervision in the *School of Computing and Electrical Engineering*, Indian Institute of Technology Mandi, and that no part of it has been submitted elsewhere for any Degree or Diploma.

Signature:

A handwritten signature in blue ink that reads "Varun Dutt". The signature is written in a cursive style and is underlined with a single horizontal line.

Name of the Guide: Dr. Varun Dutt

Date: December 8, 2020

## ABSTRACT

Attacks on cyberinfrastructure are increasing day-by-day. Due to the widespread nature of cyber-attacks and their financial consequences, there is an urgent need to focus attention on investigating how certain factors like monetary motivation (e.g., costs and benefits of actions from the attacker's and defender's viewpoint), technology constraints (e.g., how the network responds to defender's patching actions), and environmental factors (e.g., information available to players about opponent's actions and payoffs), may influence adversary's and defender's attack-and-defend decisions in the cyber world. The primary goal of this thesis is to investigate the impact of the factors mentioned above on the decisions of people performing as adversaries (hackers) and defenders (attackers) in cyber-security games using both lab-based experiments and computational cognitive models.

To understand the role of monetary motivations, three different experiments were conducted. First, the role of monetary motivations on hacker's and analyst's decisions was investigated using a security game across three different experimental setups. In the first experiment, both hackers and analysts were rewarded for attack and defend actions, respectively, and human participants performing as hackers and analysts were made to play against optimal Nash counterparts. Through these human-Nash games, human participants' deviations from their optimal proportions against their Nash counterparts were evaluated. Results revealed that, compared to the baseline, monetary rewards for human hackers and analysts caused a decline in the attack and defend actions. In addition, rewarding human hackers for undetected attacks made analysts deviate significantly from their optimal behavior. Next, another experiment was conducted to investigate the monetary motivations' role on human hackers and analysts when

human participants played against human opponents rather than Nash opponents. Results revealed that monetary motivations had a significant effect on hackers and analysts when compared to the baseline. In the third experiment on motivations, the influence of monetary penalties on analysts for their misses and false alarms was investigated. Results revealed that penalties on analysts had a significant effect on analyst's and hacker's decision-making when compared to the baseline. To understand the cognitive mechanisms that drive hackers' and analysts' decisions, computational cognitive models based upon Instance-based Learning (IBL) theory, a theory of decisions made by relying upon recency and frequency of experienced information, were developed. Results from IBL models calibrated to experimental data revealed that both hackers and analysts relied heavily upon recent and frequent information. Furthermore, IBL models were calibrated to human data collected in games involving monetary penalties on analysts. Results revealed that an IBL model that was calibrated on conditions involving monetary penalties for analysts generalized accurately to conditions involving monetary rewards for analysts and hackers.

To understand the influence of technology constraints (how the network responds to the defender's patching actions), an experiment was conducted involving Markov security games (MSGs). In MSGs, the current state of the network is determined by the last action of analyst players, and the objective of this experiment was to investigate the influence of the patching process on the attack-and-defend decisions of hackers and analysts. In an effective patching condition, the probability of the network being in a non-vulnerable state was 90% after patching by the analyst; whereas, in less-effective patching, the network's probability of being in the non-vulnerable state was 50% after patching by the analyst. Results revealed that the proportion of attack and defend actions were similar between effective and less-effective conditions.

Furthermore, although the proportion of defend actions were similar between vulnerable and non-vulnerable states, the proportion of attack actions were smaller in the non-vulnerable state compared to the vulnerable state. Most of the time, both players deviated significantly from their Nash equilibria in different conditions and states.

A cognitive model based upon IBL theory was further developed to understand the cognitive processes involved in hacker's and analyst's decisions. The model revealed low (high) reliance on recency and frequency, attention to the opponent's actions, and cognitive noise for a hacker (analyst) in effective patching. Whereas, it revealed opposite results for less-effective patching.

Finally, to understand the role of environmental factors (availability or non-availability of interdependence information), an experiment was conducted in which interdependence information (i.e., information about actions and payoffs of opponents) available to hackers and analysts was varied. In one condition, both players had complete information about each other's actions and payoffs; whereas, this information was missing in a second (control) condition. Results showed that information caused both analysts and hackers to increase their proportion of defend and attack actions, respectively. The implications of our results across monetary motivations, technology constraints, and environmental factors on cyber decision-making in the real world are highlighted.

**Keywords:** *Cybersecurity, Cognitive modeling, Defenders, Attackers, Cyber-attacks, Behavioral game theory, Instance-Based Learning Theory.*

## **Acknowledgments**

Firstly, I would like to express my sincere gratitude to Dr. Varun Dutt and Prof. V.C.S Pammi, my research supervisors, for their patient guidance, encouragement through each stage of the process. I am tremendously indebted to Dr. Varun Dutt, who instilled a research passion in me. His commitment to work deeply inspired me. Thank you, Sir, for your continued support, experience, invaluable advice, and constant motivation.

I want to offer my special thanks to the rest of my doctoral committee: Dr. Bharat Singh Rajpurohit, Dr. Renu Rameshan, Dr. Padamnabhan Rajan, and Dr. Rajendra Ray for their constructive feedback that inspired me to pursue my work from different perspectives.

I would also like to thank my fellow lab members from ACS Lab, Indian Institute of Technology Mandi (Neha Sharma, Medha Kumar, Pratik Chaturvedi, Palvi Aggarwal, Shruti Kaushik, Abhinav Chaudhry, Akash Rao), for their valuable support in lab.

I am grateful to my family for providing me moral and emotional support throughout my life. My parents Mr. Mohammad Maqbool and Mrs. Fatima for their constant encouragement, my siblings Intikhab and Mubashir for believing in me and for being the people to whom I could turn to in difficult times.

Lastly, a very special gratitude to Department of Science and Technology, India and IIT Mandi for providing me with the funding and computational requirements for my research work.

ZAHID MAQBOOL





# TABLE OF CONTENTS

THESIS CERTIFICATE

DECLARATION BY THE RESEARCH SCHOLAR

DECLARATION BY THE RESEARCH ADVISOR

ABSTRACT

ACKNOWLEDGEMENT

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

<b>Chapter 1 .....</b>	<b>1</b>
<b>Introduction.....</b>	<b>1</b>
1.1 Background.....	4
1.2 Objectives.....	8
1.3 Contribution of Thesis.....	9
1.4 Thesis Layout.....	11
<b>Chapter 2 .....</b>	<b>13</b>
<b>Theoretical and computational background .....</b>	<b>13</b>
2.1 Behavioral Game Theory (BGT) in Cybersecurity .....	13
2.2 Dynamic Security Games.....	14
2.3 Markov Security Games.....	16
2.4 Instance Based Learning Theory (IBLT) .....	19
<b>Chapter 3 .....</b>	<b>21</b>
<b>Cybersecurity: Role of monetary motivations on decision-making of attackers and defenders .....</b>	<b>21</b>
3.1 Introduction.....	21
3.2 Hypotheses.....	25
3.3 Experiment.....	27
Experiment Design.....	28
Participants.....	28
Procedure .....	29
3.4 Results.....	30
Effect of motivations on Attack and Defend Actions .....	30
Optimal proportion of Attack and Defend Actions.....	31
Proportion of Attack and Defend Actions across rounds.....	32
Correlation between Attack and Defend proportions and Demographic variables.....	35

3.5 Discussion and Conclusions.....	35
<b>Chapter 4 .....</b>	<b>38</b>
<b>Learning about Attacker’s and Defender’s Decisions via Experimentation and Cognitive Modeling in Cybersecurity Games involving Monetary Motivations .....</b>	<b>38</b>
4.1 Introduction.....	38
4.2 Role of Motivations in Cybersecurity game and Expectations on Human Behavior.....	41
4.3 Experiment.....	42
Experiment Design.....	42
Participants.....	43
Procedure .....	43
Hypotheses.....	44
4.4 Results.....	44
Proportion of Attack and Defend Actions.....	44
Proportion of Attack and Defend Actions across rounds.....	46
4.5 Instance-Based Learning Theory (IBLT) and IBL Model .....	49
Implementation and Execution of IBL Model in Cybersecurity Game .....	52
Model Results .....	52
4.6 Discussion .....	53
<b>Chapter 5 .....</b>	<b>56</b>
<b>Cybersecurity: Effects of Penalizing Defenders in Cybersecurity Games via Experimentation and Computational Modeling .....</b>	<b>56</b>
5.1 Introduction.....	56
5.2 Effect of Monetary Penalties in Cybersecurity Game.....	58
5.3 Experiment.....	61
Experimental Design.....	61
Stimulus and Apparatus .....	61
Participants.....	62
Procedure .....	63
Hypotheses.....	63
5.4 Results.....	64
5.5 IBL Model.....	65
Calibration of Model Parameters .....	66
IBL Model Generalization .....	68
5.6 Discussion and Conclusions.....	72
<b>Chapter 6 .....</b>	<b>76</b>

<b>Cybersecurity: Investigating the Influence of Patching Vulnerabilities on Cyber Decision-making via Cognitive Modeling.....</b>	<b>77</b>
6.1 Introduction.....	77
6.2 Hypotheses.....	80
6.3 Experiment.....	81
Participants.....	81
Experimental Design.....	82
Procedure.....	83
6.4 Experimental Results.....	84
Proportion of Attack and Defend Actions.....	84
Proportion of Attack and Defend Actions across States.....	85
Proportion of Attack and Defend Actions across Patching Conditions and States.....	86
6.5 IBL Models for Attackers and Defenders.....	87
Models' Execution Procedure.....	88
Model Results.....	89
Calibrated Parameters of the Model.....	91
6.6 Discussion and Conclusions.....	92
<b>Chapter 7.....</b>	<b>96</b>
<b>Cybersecurity: Effect of Information Availability on Decision-making of Attackers and Defenders in Cybersecurity Games.....</b>	<b>96</b>
7.1 Introduction.....	96
7.2 Influence of Interdependence Information and Expectations on Human Behavior.....	98
7.3 Experiment.....	100
Participants.....	101
Procedure.....	101
Hypotheses.....	101
7.4 Experimental Results.....	102
Proportion of Attack and Defend Actions.....	102
Proportion of Attack and Defend Actions across rounds.....	102
7.5 Discussion and Conclusions.....	104
<b>Chapter 8.....</b>	<b>106</b>
<b>Conclusion and Future Scope.....</b>	<b>106</b>
8.1 Conclusion.....	106
8.2 Research Implications.....	110
8.3 Limitations.....	112

8.3 Future scope .....	112
<b>List of Publications from Thesis .....</b>	<b>126</b>
<b>List of Other Publications .....</b>	<b>128</b>