Attacking and defending perspective of e-Crime behavior and psychology: A systemic dynamic simulation approach

Deng-Yiv Chiu
Professor, dept. of Information Management
Chung-Hua University /Hsin Chu City, Taiwan
Email: chiuden@chu.edu.tw

Chen-Shu Wang
Assistant Professor, graduate Institute of Information and Logistics Management
National Taipei University of Technology /Taipei , Taiwan
Email: jenny6508@seed.net.tw

Tien-Tsun Chung
Ph. D. Student, dept. of Information Management
Chung-Hua University /Hsin Chu, Taiwan
Email: e09410019@chu.edu.tw

***Abstract*—Cybercrime is a worsening problem that can lead to loss of financial and personal information. However, e-crime is particular hard to detect since internet is boundless that make evidence hard to collect. Additionally, compare to others crime issues, e-crime is an emerging crime type thus previous crime theories should be refined and new methods of predicting e-crime should be further developed. In this research, we constructed a system dynamic simulation model from both e-crime attacking and defending side respectively. Various decision variables that related to behavior and psychology perspectives of victim and offender were added to proposed model. Furthermore, the actual e-crime data of Taiwan from Year 2000 to 2008 for cyber fraud (CF) and offend computer usage (OCU) are then further verified the proposed model. As the simulation result demonstrated, the accuracy rate of e-crime predication can be achieved about 80%. Additionally, some interest parameters are also revealed, such as the recidivism rate and report rate of victim were unknown in previous research. Finally, via inference of simulation result, some suggestions are also proposed to reduce potential e-crime behavior.**

I. INTRODUCTION

Cybercrime, also known as e-Crime, is a worsening problem that can lead to loss of financial and personal information [4]. Online users are becoming cautious and anxious when operating ICT (Information Communication Technology) equipment [11]. Generally, cybercrime refers to cyber fraud (CF), violations of privacy rights and sexual crimes. According to the definition proposed in Brenner & Schwerha (2004) [2], e-crime behavior through ICT equipment has been an emerging issue since 1994. However, e-crime is particular hard to detect or prevent since internet is boundless across country and international laws make evidence hard to collect [10].

In Taiwan, the 9th Investigation Brigade of Provincial Police Division report for January to July 2008 indicated that of 12,007 e-crime related issues, 41.5% were cyber fraud, 16.8% were offense of computer usage (OCU), and 15.6% and 9.4% were violations of the Child and Youth Sexual Transaction Prevention Act Law and sexual offenses laws, respectively. Further, 11.2% were related to privacy right violations. Obviously, the majority (58%) e-crime issues in Taiwan are related to cyber fraud (CF) and offense of computer usage (OCU) crime behavior. Additionally, there is particular CF and OCU crime behavior of Taiwan, named treasure stealing of computer game, differs from that in other countries. Because online gaming is popular in Taiwan and usually exist various highly value of virtual treasures and tokens in game scenario, stealing or cheating to obtain treasure or tokens is a common e-crime issue related to CF and OCU. Nevertheless, many OCU offenders claim that their intent is to obtain a virtual object (such as virtual treasure or game tokens); they do not believe that their actions harm anyone. Therefore, e-crime is a becoming serious issue that should be addressed.

Researchers in criminal psychology and behavior have developed many crime theories to explain this phenomenon. For example, crime opportunity theory suggests that humans intend to committee a crime, but the crime intention can be restricted by willpower. Additionally, the crime-opportunity is decided by exogenous environment variables such as crime-punishment law and the success rate. If opportunities to commit crimes are reduced, and if the willpower of potential offenders is decreased, crime can be reduced. On the other hand, according to society control theory proposed by Hirschi (1969) [7], personal sanctions against crime are related to the connection between society and individual. Criminal behavior is negatively

doi:10.4304/jsw.5.12.1349-1354

related to personal sanctions, which consist of commitment, involvement, belief and attachment. Conversely, Cohen & Felosn (1979) proposed the theory that criminal behavior is a common activity including motivation [5], object and protect. Almost all previous studies explored decision variables that decided and affected crime behavior from various perspectives. However, for e-crime behavior, an emerging crime type that relies on IT technologies to complete, some decision variables based on crime theories proposed by previous researches may not adequately explain the e-crime behavior of today. For example, society control theory addresses how the connection between society and individual reduces crime behavior. However, the connection is ambiguous for e-crime condition because the internet is boundless, and the criminal may even have a virtual role. Thus, according to social control theory, sanctions for crimes are related to society, and individual connections are difficult to evaluate for e-crime issue [9].

Recently, Hinduja (2008) discussed Internet privacy behavior from an applied deindividuation theory perspective which analyzed network characteristic (such as anonymity and rapid data transfer rate) to demonstrate how easily intelligence privacy was violated[7]. When discussing e-crime, it is much more reasonable to consider networking characteristics because the e-crime location is a network, and the crime is completed by IT technologies. Thus, to address e-crime issues, previous crime theories should be further revised and applied appropriately. Furthermore, e-crime is a dynamic and complex problem, which makes criminal behavior difficult to predict. For example, the e-crime rate may be negatively related to strict degree with punishment law (as punishment for e-crime becomes more severe, the e-crime rate should become lower), but the rate of e-crime is positively related to emerging IT technologies (emerging IT technologies reduce the risks and difficulty of crimes and thus increase the e-crime rate). Therefore, e-crime behavior is dynamic, complex and hard to predict by a single variable. A systematic perspective is needed. To address e-crime issues, previous crime theories should be refined, and new methods of predicting e-crime should be further developed.

This study analyzes e-crime in Taiwan from a systematic perspective, including offender psychology and behavior. The primary goals of this research are the followings:

(1.) Most (58%) e-crimes in Taiwan are cyber fraud (CF) and offense of computer usage (OCU). Therefore, a systematical dynamic model must first be established for these two e-crime behaviors. The proposed model can then be used to analyze other e-crimes.

(2.) Additionally, four dynamic hypotheses are tested via simulation result. First, the relationships among police manpower and quality and the propaganda effect of legislation and e-crime behavior are analyzed. Further, some interesting but unknown parameters (such as report rate by e-crime victim and recidivism rate of offender) are also revealed by the simulation.

(3.) Finally, some recommendations are proposed for e-crime behavior decrease and prevention.

The remainder of this paper is organized as follows. Section 2 details the proposed system dynamic (SD) simulation model, and Section 3 then presents the simulation results of the proposed SD model. Conclusions are finally drawn in Section 4 along with recommendations for future research.

II. Systematical Dynamic Simulation Model for E-Crime

Similar to all crimes, e-crime can be classified as defending or attacking [8]. According to crime opportunity theory, the potential offender evaluates the crime behavior success rate, and that crime opportunity is compared with the intensity of defending and attacking where the offender is considered the attacking side, and the police are the defending side. Figures 1 and 2 show the two parts of the dynamic simulation model, the defending side and the attacking side, respectively.

Figure 1 details the defending side of the e-crime SD simulation model. Clearly, the investigative abilities of the police are affected via policy a capability that consists of investigation equipment operator skill capabilities which then affects e-crime solving rate. Lamentably, an offender detected and captured by the defending side may be a recidivist and transfer to the attacking side again. Table 1 shows decision variables that may affect the defending side according to previous studies. For illustration, Chung et al., (2006) claimed various approaches[3], including: legal, organization and technology can decrease cyber crime efficiency. Additionally, according to criminal opportunity theory, the following two dynamic hypothesizes can be reasonably inferred:

H1: Police manpower and quality are positively related to the e-crime solution rate.

H2: The propaganda effect of legislation is negatively related to the e-crime rate.

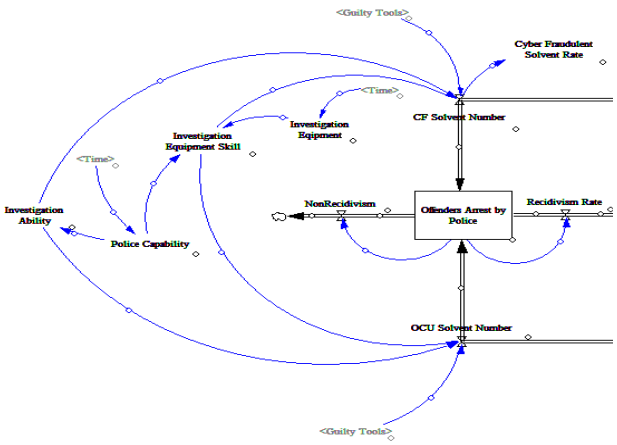

Figure 1. The defending side of e-crime simulation model

In detail, criminal opportunities decrease as policies manpower increases because the enhanced investigative ability may improve the solvent rate. Thus, H1 is expected to be supported. Additionally, H2 proposes that the propaganda effect is negative related to the e-crime rate because some offenders claim they do not know their behavior violates e-crime law. Thus, we believe the legislation propaganda effect is negatively related to crime behavior, but there would be a period time delay because of the advertising effect may spread by word-of-mouse. Therefore, H2 should be 5 supported, and the e-crime rate should decrease.

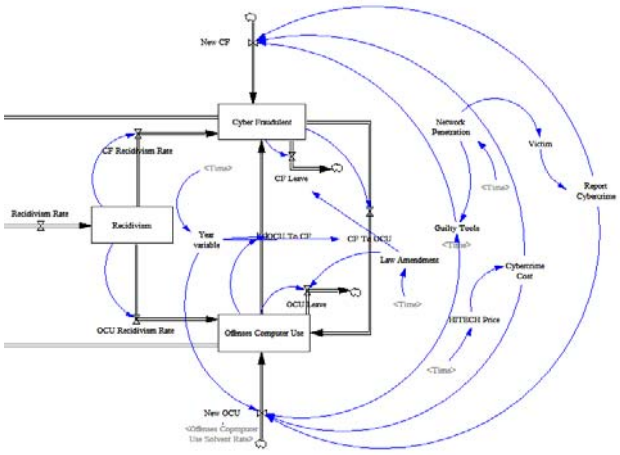

Figure2. Attacking side of e-crime simulation model

For the attacking side, Fig. 2 displays the relationship among decision variables listed in Table 1. In Taiwan, the available network penetration rate in the second quarter of 2008 averaged 44%. Therefore, a positive association between e-crime behavior and network penetration rate is expected because e-crime is completed via network and other ICT equipment. Thus, dynamic hypothesis 3 is proposed:

H3: Network penetration rate is positively related to e-crime.

H4: Actual e-crime rate significantly differs from reported e-crime rate.

Except for CF and OCU, amounts are regarded as indicator variables for evaluating model accuracy. Table 1 shows three further indicators: report rate, recidivism rate and transfer rate. For report rate, victims of e-crime may not file police reports due to embarrassment, fear of retaliation by the offender, or, in the worst case, unawareness that the crime has occurred. The local police may consider the loss from e-crime to be too small to investigate further. Thus hypothesis 4 is proposed. The e-crime report rate is an interesting but unreported parameter in previous research. Additionally, recidivism rate is another important parameter for evaluating defending side performance because, as recidivism rate decreases, e-crime should decrease or even disappear. Finally, previous research indicates that the transfer rate between e-crime types is always an unaddressed

TABLE I.
VARIABLE DEFINITION

Decision variable	Description	Based on
	Defending Side	
e-Crime solvent rate	The police ability to detect and solve e-crimes.	[5]、[6]
Investigation equipment	To detect e-crime behavior, specialized hardware (e.g., sniffers) and software is required.	[3]、[5]
Police capability	To deal with emerging e-crime behavior, police require further investigative training and skill in equipment operation.	[3]、[5]
Legislation propaganda effect	As the e-crime regulations revision and accompany with appropriate propaganda enable people better understanding e-crime.	[3]、[6]
Investigation ability	To investigate e-crimes, police require basic understanding of network concepts	[5]
	Attacking Side	
Crime tools	e-crimes involve networking and IT equipment. Thus, emerging software and hardware must be considered.	[5] 、[6]
e-crime cost	Because tools for e-crime are mostly ICT equipment, emerging IT is considered the e-crime cost.	[5]
Network penetration	Continuous network penetration is expected and is positively related to e-crime.	[1]
	Indicator variable	
Cyber fraud & Offend computer use crime issue	These two crimes (CF & OCU) increased from 2000 to 2008 and are indicators for evaluating the proposed model	
e-Crime report rate	This e-crime report rate parameter represents whether victimsreport e-crimes to the police, is difficult to evaluate.	
Recidivism Rate	Recidivism transfers offender from the defending side toattacking side.	
Transfer rate	e-crime transformation among e-crime types such as from CF toOCU or OCU to CF.	

parameter of e-crime transformation such as CF to OCU or OCU to CF. Generally, OCU is a predecessor crime of CF. Thus, the transfer rate for predicting serious e-crime rate (OCU to CF) can be observed, and the transfer rate can also be considered defending side performance (e.g., legislation propaganda effect preventing potential offenders from committing serious crimes).

III. SIMULATION RESULTS

To verify the proposed model for e-crime structure, actual e-crime statistical data was used in the simulation. High performance system and free open source Vensim® (1994) software was used to model development and simulation. The Appendix lists related equations. The simulations analyzed 121,284 e-crime related issues, including 19,273 cyber fraud issues (from 1999 to September, 2008) and 47,803 related to offences of computer usage (from 2004 to September, 2008). The existing OCU trend is represented by the blue line in Fig. 3. The OCU crimes peaked in 2005 and then dramatically decreased, probably due to the legislation were renounced in 2003 and the propaganda effect which was observed 2 years later. Thus, H2 was supported that time delay effect is existing. The finding is consistent with Chung et al., (2006) conclusion [3].

The simulation results for CF from 1999 to 2007Additionally, as Figs. 3 and 4 indicate, two indicator

variables were accumulated OCU and CF crime issues. Both variables were compared to actual e-crime data. For OCU & CF crime, the accuracy prediction rate was 90.61% and 71.48%, respectively, indicating that H1 and H3 were significant supported. Therefore, the decision variables listed in Table 1 adequately indicated defending and attacking sides and their interaction.

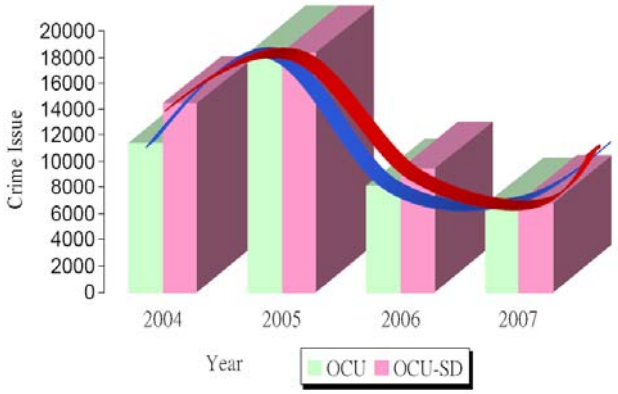

Figure3. The simulation results for OCU from 2004 to 2007

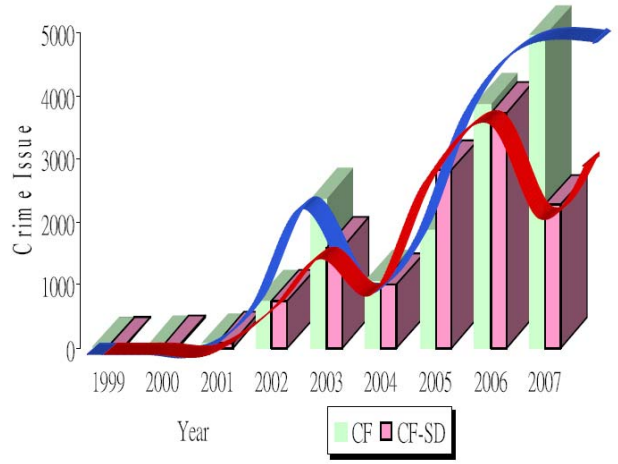

Figure4. The simulation results for CF from 1999 to 2007

TABLE II.
SIMULATION RESULT FOR CYBER CRIME PARAMETER

Parameter	Simulation Result
e-crime report rate from victim	20%
Recidivism rate	30% (24% for CF, 6% for OCU)
e-crime transfer rate	6% CF to OCU and 15% OCU to CF

Finally, other indicator variables were also revealed via simulation result in Table 2. The recidivism rate was about 30% but the 80% and 20% in CF and OCU respectively, was consistent with expert opinion which CF has a higher recidivism rate (about 24%) than OCU (about 6%). Further, the transfer rate of CF to OCU was 6%, and that of OCU to CF was 15% because of the crime issue is usually becoming serious as the OCU offenders do not catch by defense side (such as police). Additionally, the simulation results also revealed that the e-crime report rate was about 20%, meaning that 80% of victims do not report e-crimes, which supports H4. But, that is an anxiety issue that about 5 times e-crime occurrence but not mentioned because of only 20% e-crime issues reported to police. These parameters are important but are always regarded as expert knowledge which is hard to verify. Therefore, the simulation can compensate for this disadvantage.

IV. CONCLUSION AND FURTHER WORKS

e-Crime is worsening and the growing use of the Internet ensures further dramatic increases. This research developed a simulation model to identify decision variables and relative parameters affecting e-crime behavior from an attacking-defending perspective. As the simulation demonstrated, the accuracy rate for the proposed simulation model averaged 80%; thus, the discussed decision variables were significant to represent e-crime issue structure. Further, some interesting parameters were also revealed via simulation, such as the recidivism rate (30%) and the report rate (20%). These parameters are also consistent with domain experts (Internet police) and consistent with their opinion and practice experience.

The proposed simulation model is a systemic model that provides decision makers with a complete vision for e-crime psychology and behavior. Hence, decision makers and possibly lawmaking committees can reference the simulation results and take appropriate action. For example, the simulation results reveal that legislation propaganda effect is inversely related to OCU crime; thus the budgets for relative law-revision popularization can possible approach to decrease OCU. Additionally, CF crime can also be expected to decrease due to the 6% transfer rate of e-crime type (from OCU to CF). To reduce e-crime, for defending side, the simulation results also suggest enhancing capability through operation training in investigative tools. For the attacking side, as new IT hardware and software emerges, e-crime issues can be expected to increase because of e-crime costs decrease and technology upgrades usually existing unexpected problem that makes upgraded technology may be attacking easily (such as new version operation system should be repaired via service pack). Thus, the defending side should address dramatic crime issue at particular timing (such as new version OS announced).

To address e-crime issues effectively, the psychology and behavior of victims and offenders should be further probed. For example, the report rate of e-crime victims (only 20%) is lower than expected and should be discussed further. The decision variable that affects recidivism rate of offenders is also an interesting direction for further research. The accuracy of the proposed model can be enhanced further and applied to all e-crime issues.

APPENDIX A APPENDIX TITLE

A. CF Leave= (Cyber Fraudulent*Law Amendment)*0.1
B. CF Recidivism Rate=DELAY3(Recidivism*0.8,1)
C. CF Solvent Number=((Investigation Ability*Investigation Eqipment Skill*3)/(Guilty Tools*0.3))*Cyber Fraudulent
D. CF To OCU=(Cyber Fraudulent*0.06)*Year variable
E. Cyber Fraudulent= INTEG (New CF+CF Recidivism Rate + OCU To CF-CF To OCU-CF Leave-CF Solvent Number,1)
F. Cyber Fraudulent Solvent Rate=CF Solvent Number/Cyber Fraudulent
G. Cybercrime Cost=100000/HITECH Price
H. FINAL TIME = 96 The final time for the simulation.
I. Guilty Tools=IF THEN ELSE(Time>89 , Network Penetration*15 ,Network Penetration*1.5)
J. HITECH Price = WITH LOOKUP (Time, ([(88,0)-(96,80000)], (88,70000), (89,65000), (90,55000), (91,52000),(92,40000),(93,35000),(94,30000),(95,25000),(96,20000)))
K. INITIAL TIME = 88 The initial time for the simulation.
L. Investigation Ability=Police Capability
M. Investigation Equipment = WITH LOOKUP (Time, ([(88,0)-(96,1)], (88,0.1), (89,0.1), (90,0.4), (91,0.45), (92,0.5),(93,0.5),(94,0.6),(95,0.75),(96,0.75)))
N. Investigation Equipment Skill=Investigation Equipment * Police Capability
O. Law Amendment = WITH LOOKUP (Time, ([(88,0)-(96,1)], (88,0), (89,0), (90,0), (91,0), (92,0), (93,0.1),(94,0.6),(95,0.7),(96,0.7)))
P. Network Penetration = WITH LOOKUP (Time, ([(88,0)-(96,1)], (88,0.22), (89,0.28), (91,0.38), (92,0.39),(93,0.4),(94,0.42),(95,0.43),(96,0.44)))
Q. New CF=((Cybercrime Cost*Guilty Tools/DELAY3(Cyber Fraudulent Solvent Rate,1))*(Report Cybercrime*0.03))
R. New OCU= ((Report Cybercrime*0.15)*(Cybercrime Cost*Guilty Tools/(Offenses Computer Use Solvent Rate)))*Year variable
S. NonRecidivism= Offenders Arrest by Police*0.7
T. OCU Leave=(Offenses Computer Use*Law Amendment)
U. OCU Recidivism Rate= DELAY3(Recidivism*0.2 , 1)
V. OCU Solvent Number= ((Investigation Ability*Investigation Equipment Skill)/(Guilty Tools))*(Offenses Computer Use)
W. OCU To CF=Offenses Computer Use*0.15*Year variable
X. Offenders Arrest by Police= INTEG (OCU Solvent Number + NonRecidivism+ CF Solvent Number +Recidivism Rate,0)
Y. Offenses Computer Use= INTEG (OCU Recidivism Rate+ New OCU+CF To OCU-OCU To CF-OCU Solvent Number-OCU Leave,1)
Z. Offenses Computer Use Solvent Rate= OCU Solvent Number/Offenses Computer0020vUse
AA. Police Capability = WITH LOOKUP (Time, ([(0,0)-(100,10)], (88,0.1), (89,0.1), (90,0.4), (91,0.4),(92,0.4),(93,0.6),(94,0.75),(95,0.8),(96,0.8)))
BB. Recidivism= INTEG (Recidivism Rate-OCU Recidivism Rate-CF Recidivism Rate, 0)
CC. Recidivism Rate= Offenders Arrest by Police*0.3
DD. Report Cybercrime=Victim*0.2
EE. SAVEPER = TIME STEP The frequency with which output is stored.
FF. TIME STEP = 1 The time step for the simulation.
GG. Victim= (Network Penetration*2.3e+007)*5e-005
HH. Year variable = WITH LOOKUP (Time, ([(88,0)-(96,1)], (88,0), (89,0), (90,0), (91,0), (92,1), (93,1), (94,1),(95,1),(96,1)))

REFERENCES

[1] Beck, U., Der Konflikt der zwei Modernen, in: demselben: Politik in der Risikogesellschaft. Frankfurt/M., 1991, pp. 180-195.
[2] Brenner, S., and Schwerha IV, J., "Introduction-Cybercrime: A Note on International Issues," Information Systems Fontiers, Vol. 6, No. 2, 2006, pp. 111-114.
[3] Chung, W., Chen, H., Chang, W., and Chou, S., "Fighting Cybercrime: A Review and the Taiwan Experience," Decision Support Systems, Vol. 41, No. 3, 2006, 669-82.
[4] Cymru, T., "Cybercrime-An Epidemic," ACM Queue, Vol. 9, No. 4, 2006, 25-28.
[5] Cohen, L.E., and Felson, M., "Social Change and Crime Rate Trends: A Routine Activity Approach," American Sociological Review, Vol.44, 1979, pp.588-608.
[6] Hirschi, T. Causes of Delinquency (Transaction Publishers 2002 edition ed.), 1969, Berkeley: Unversity of California Press.
[7] Hinduja, S., "Deindivididuation and Internet Software Piracy," CyberPsychology & Behavior, Vol. 11, No. 4, 2008, pp. 391-398.
[8] O'Hanlon, C., "The Criminal Mind," ACM Queue, Vol. 9, No. 4, 2006, pp. 7.
[9] Stephens, G., "Cybercrime in the Year 2005," The Futurist, 2008, pp. 32-36.
[10] Wadlow, T., and Gorelik, V., "The Making of a Cybercriminal," ACM Queue, Vol. 9, No. 4, 2006, pp. 25-28.
[11] Wolak, J.D., Finkelhor, D., and Mitchell, K., "Is Talking Online to Unknown People Always Risky? Distinguishing Online Interaction Styles in a National Sample of Youth Internet Users," CyberPsychology & Behavior, Vol. 11, No. 3,2008, pp.340-343.

Deng-Yiv Chiu received the B.A. from Averett College, Virginia, USA in 1988, M.S. from University of Maryland, USA in 1990. He received the Ph.D. in Computer Science from Illinois Institute of Technology, USA in 1994. After working as an assistant professor at Dept. of Math and Computer Science, Chicago State University, USA and as a system analyst at John Deere, Inc., USA, he has been an associate

professor/ full professor at Chung Hua University, HsinChu, Taiwan since 1996. His research interests include machine learning, information retrieval, and their applications to knowledge management and finance. contain a place and/or date of birth (list place, then date). Next, the author's educational background is listed. The degrees should be listed with type of degree in what field, which institution, city, state or country, and year degree was earned. The author's major field of study should be lower-cased.

Chen-Shu Wang received bachelor degree in management information system from national Yunlin University of science & technology in 2000 and M.S. Degree of National Chang-Hwa university of education in 2003. Now, she is an assistant professor at graduate Institute of Information and Logistics Management of National Taipei University of Technology. Her research interests focus on AI Technologies integration and application, Simulation optimal and organization strategic.

Tien-Tsun, Chung is a Ph. D. student in the Information Management Dept, Chung-Hua University, Taiwan. His research interests are System Dynamics and Data Mining.
e-mail: e09410019@chu.edu.tw