A Historical Review of Computer User's Illegal Behavior Based on Containment Theory

Chi-Chao Lu
Overseas Chinese University/Center for General Education, Taichung, Taiwan
Email: chichao@ocu.edu.tw

Wen-Yuan Jen
National United University/Institute of Information and Society, Taichung, Taiwan
Email: wyjen@nuu.edu.tw

***Abstract*—The aim of this study is to explore research trends in computer crime and cybercrime from 1968 to 2009. The findings of the current study will provide some insight into scholarly activity related to computer crime and cybercrime and will be useful in tracking computer user's illegal behavior research trends. Our other goal is to explore the range of the theoretical lens that can be used to understand social controls in restraining computer user's illegal behavior intention. Towards this goal, this study proposed five propositions based on containment theory. Our propositions address social control education, and offer insights in restraining computer user's illegal behavior intention.**

***Index Terms*—containment theory; computer crime; cybercrime; social control, user illegal behavior.**

I. INTRODUCTION

Many literatures and researches are endeavored to increase the multiple functions and services between computer and human [1-4]; however, few studies have examined the occurrences of illegal computer acts and theoretical explanations for the computer user's illegal behavior [5-7] are needed in global cyber society. Due to an increase in Internet users and the growth of e-commerce as an important business model, the number of illegal cases has risen dramatically, and the U.S. Federal Bureau of Investigation (FBI) reports that cyber criminals have attacked almost all of the Fortune 500 companies [8]. Not all cybercrime involves property loss. The Internet has also changed human relationships and behavior as well, and cybercrime also takes the form of sexually-related Internet crime [9], game addiction [10-11], and hacking behavior [12]. Clearly, the illegal behaviors are issues worth discussing. An evaluation of the distribution and scope of related scholarly papers published worldwide will be helpful in understanding the trends in computer user's illegal behavior research.

Bell [13] defined computer crime as "an offence in which a computer network is directly and significantly instrumental in the commission of a crime." Thomas and Loader [14] defined cybercrime as "illegal computer-mediated activities that often take place in the global electronic networks." Both computer crime and cybercrime are related to illegal behavior or criminal activity. Over the last three decades, computers and computer networks have played an increasingly indispensable role in people's lives. However, both computers and computer networks have also created a new venue for criminal activity, and cybercrime and cyber terrorism have risen to the FBI's number three priority, behind counterterrorism and counterintelligence [15]

Guzman and Kaarst-Brown [16] adopted content analysis to analyze published research on skill expectations and contributions to organizational survival and strategic alignment of IT. In order to do the historical review in research trends in computer user's illegal behavior and social control, a longitudinal literature review is indispensable. Hence, this study explores the issues based on the Web of Knowledge Database of Institute for Scientific Information (ISI).

The paper is organized as follows. First, methods and materials are presented. Next, employing the ISI Web of Science, Publications were analyzed and evaluated for a longitudinal literature review, and a historical review was also performed. Next, an overview of computer user's illegal behavior is discussed based on containment theory. In this paper, the study findings may be found useful in following research trends.

II. REVIEW OF RELEVANT LITERATURES

Some sociological theories address why people become criminals, but while others don't. In this study, containment theory [17] is employed to explore the computer user's illegal behavior. Containment theory [17-18] assumes that for every individual a containing external structure as well as a protective internal structure exists. Reckless [17] pointed out that people by nature behave in accord with their self-interest and are inclined to violate rules unless they are constrained. Containment theory adapts social bonding and control theory by suggesting that people are prevented from committing crimes because of various "outer containment" and "inner containment" conditions [19]. In essence, containment theory explains criminal behavior as the interplay

Corresponding author: Wen-Yuan Jen
No.1, Lien Da, Miao-Li, Taiwan
Tel: +886-37-381872
Fax: +886-37-381857

doi:10.4304/jsw.5.6.593-599

between two forms of control known as inner containment and outer containment.

Inner containment is the containment defined by an individual's norms and values, such as morality, ego, and conscience. An individual's behavior is controlled by inner containment, and when the individual goes beyond a norm, he/she feels guilty or sorry. Outer containment conditions include preventative measures and supervision, tantamount to a reduction in crime opportunity, or an increase in the degree of difficulty of committing the crime; strong group cohesion; and consistency of morality [19]. Outer containment is defined by two forms: (1) Informal external social control, such as informal sanctions by parents and peers, and (2) Formal external social control, such as legal sanctions by the legal environment (e.g., laws, legislation and government). The individual conforms in order to keep his/her freedom, position, money or reputation; hence people behave under outer containment.

Computer user's behavior is not limited to the scope of single user and one computer; conversely computer user's behavior is various. Bandura [20-21] explains human behavior in terms of continuous reciprocal interaction between cognitive, behavioral, and environmental influences. Hence, computer user's behavior is affected by individual's cognitive, behavioral, and environmental influences. The same way happened to computer user's illegal behavior. According to containment theory, inner containment and outer containment are both factors to affect the trends of computer user's illegal behavior as well.

III. Methods and Materials

Content analysis is the quantitative evaluation of scientific literature. Krippendorf [22] defined content analysis as a research technique for making replicable and valid references from data to corresponding context. Researchers are able to identify structured and patterned regularities in the text and make inferences on this basis.

The *Web of Knowledge* database of the Institute for Scientific Information (ISI) includes information from over 22,000 journals covering more than 230 scientific disciplines. ISI *Web of Science* includes SCI, SSCI, and A&HCI. This study employed ISI databases included in the online version of the ISI *Web of Science*. In this study, "computer crime" and "cyber crime" were used as keywords to search "title," and "topic" fields of the ISI databases. In using the online ISI *Web of Science*, this study set the time span from 1900 to 2009. On August, 2009, there database search produced 415 documents related to computer crime and 53 documents related to cybercrime. Examining these results, we found the first computer crime paper was published in 1968; hence, the time span of this study was defined as being from 1968 to 2009.

For a longitudinal literature review, we not only employed content analysis to do historical review of computer user's illegal behavior, but also proposed five propositions based on containment theory.

TABLE I. PUBLICATION YEAR DISTRIBUTION (TOP 10)

Computer crime			Cybercrime		
Publication Year	Record Count	% of 415	Publication Year	Record Count	% of 53
2007	30	7.23%	2006	9	16.98%
2009	28	6.75%	2007	8	15.09%
2004	24	5.78%	2001	7	13.21%
2005	21	5.06%	2003	6	11.32%
2006	21	5.06%	2008	6	11.32%
1984	20	4.82%	2005	4	7.55%
2008	20	4.82%	1998	3	5.66%
2003	18	4.34%	2000	3	5.66%
1995	17	4.10%	2004	3	5.66%
1993	14	3.37%	1999	2	3.77%

TABLE II. DOCUMENT TYPE DISTRIBUTION (TOP 5)

Document type	computer crime		cybercrime	
	Record Count	%of 415	Record Count	%of 53
Article	267	64.34%	36	67.92%
Proceedings paper	40	9.64%	8	15.09%
Editorial material	36	8.68%	4	7.55%
Book review	27	6.51%	3	5.66%
News item	14	3.37%		

IV. Results and Discussions

There were a total of 415 documents in the computer crime and 53 documents in the cybercrime literature during the period 1968-2009. Table I displays top 10 publication year distribution. In computer crime, the first paper was published in 1968; in cybercrime, the first paper was published in 1998. Due to the significance of user's illegal behavior, the number of documents produced annually is expected to grow.

From Table II, we see that among the reviewed ISI database documents, the distribution of document types was scattered in computer crime, with articles constituting a majority of all documents. In computer crime, the document types were dominated by articles (267, 64.33%) and proceeding paper (40, 9.64%). In cybercrime, the document types were dominated by articles (36, 67.92%) and proceeding paper (8, 15.09%). In addition, ISI databases shown that English was the major language of publication for computer crime and cybercrime.

A detailed analysis of authors' countries, Table III, reveals that most papers originated in the USA, with England, Germany, Canada, Taiwan, and Australia following. With regard to distribution of articles by country, the results show that the USA took the lead

TABLE III. COUNTRY DISTRIBUTION (TOP 5)

Computer crime			Cybercrime		
Country	Record Count	% of 415	Country	Record Count	% of 53
USA	178	42.89%	USA	20	37.74%
ENGLAND	42	10.12%	TAIWAN	5	9.43%
AUSTRALIA	9	2.17%	ENGLAND	4	7.55%
CANADA	9	2.17%	AUSTRALIA	3	5.66%
GERMANY	9	2.17%	CANADA	3	5.66%

TABLE IV. JOURNALS CONTAINING MOST PAPERS (TOP 5)

Computer Crime Source Title	No. Papers	% of 415	Cybercrime Source Title	No. Papers	% of 53
Computers & Security	26	6.27%	Computers & Security	6	11.32%
KRIMINALISTIK	22	5.30%	Computer standards & Interfaces	4	7.55%
Digital investigation	10	2.41%	Digital investigation	4	7.55%
Data management	9	2.17%	Lecture notes in computer science	4	7.55%
IEEE spectrum	9	2.17%	Crime law and social change	3	5.67%

among countries in both computer crime and cybercrime categories. In computer crime, the journal 'Computer & Security' contained the most articles and the major subject category was "Criminology and Penology". In cybercrime, the journal 'Computer & Security' contained the most articles and the major subject category was "Computer Science, Information Systems". This is not surprising, as *Computers & Security* has been devoted to the field of computer crime and cybercrime for many years. More detail information is listed in Table IV.

The analysis of the development of Internet, outer containment and inner containment reveal the developments of the computer user's illegal behavior past three decades. More detailed delineation is following.

A. The development of Internet

Table V illustrates the development of the Internet [23] and summarizes the focus of computer crime and cybercrime literature in each decade. In the final year of the Internet implementation stage (1961-1974), the first computer crime paper was published. In the Internet institutionalization stage (1975-1993), the period from 1975 to 1980 saw the most publications focusing on the innate character of computer crime. For instance, the analysis of computer crime types and causes were major issues during that period. From 1981 to 1990, a legal focus dominated, and computer crime legislation issues were explored.

In 1994, the first web browser, Netscape, was made available to the general public, and Internet business applications emerged. Web browser development then led to the Internet being commercialized and computer crime entered a concomitant growth period.

B. The development of outer social control

According to Containment theory, people don't commit illegal behavior because of various "outer containment" and "inner containment" conditions. Dhillon et al. [24] suggests that organizations are most likely to prioritize control strategies in the following order: technical controls, formal controls, informal controls. *Technical controls* are defined by technical devices or settings (e.g. firewalls, password protection, encryption and others) which work for reducing crime commission opportunities. As Table VI shows, information security and opportunity/control were developed. *Formal controls* are organizational measures which outline acceptable behavior and organizational structure which defines responsibilities, adequate supervision, and related responsibilities. As Table VI shows, insider and organization related policies were developed. Such *Technical controls and Formal controls* correspond to containment theory's outer controls.

Law legislating, forensic science and digital evidence

TABLE V. HISTORY OF FOCUS POINTS OF COMPUTER USER'S ILLEGAL BEHAVIOR LITERATURE

Decade	Computer crime	Cybercrime	Internet development
1968-1970	▪ The issue was focus on computer against crime.		1961-1974 Internet implementation stage
1971-1980	▪ Computer crime types, causes, and investigation were discussed in this stage.		
1981-1990	▪ Computer crime legislation and prevention demands of computer crime for business were increased. ▪ Computer crime pattern analysis and hacker behavior began to be discussed.		1975-1993 Internet institutionalization stage
1991-2000	▪ Forensic-science against computer crime legislation updated. ▪ Behavioral issues were explored ▪ Information security issues were emerging.	▪ The stage focused on cybercrime forensics and the impacts caused by cybercrime.	1994 1st web browser – Netscape entered market, and started electronic commerce.
2001-2009	▪ Various dimensions related to computer crime were discussed	▪ Information security issues were increased. ▪ Law enforcement and legislation updated.	1995-present Internet commerce stage

TABLE VI. TWO CONTAINMENTS OF COMPUTER USER'S ILLEGAL BEHAVIOR

Containments	Items	Contents	Author(s)
Outer containment	Technical control	Information security	Chang, et. al. [25]; Huang [26]; McMullan and Perrier [27]
		Opportunity/control	Willison and Backhouse [28]; Dhillon and Moores [29]
	Formal control	Insider/employee	Higgins [30]; Haugen and Selin [31]
		Policy	Foltz, et. al. [32]; Groenhuijsen and Schudelaro [33]
	Law enforcement	Law legislating	Burns, et. al. [34]; Brenner [35]; Mendez [36]
		Forensics	Kao, et. al. [37]; Arnes, et. al. [38]; Kim, et. al. [39]; Rogers and Seigfried [40]
Inner containment	Informal control	Ethical issues/ Attitude/awareness	Harrington [41]; Cordeiro [42]; Udas, et. al., [43]; Dowland, et al. [44]
		Self-control	Higgins and Makin [45]; Higgins [30]
		Illegal behavior studies	Cronan, et. al. [46]; Limayem, et. al. [47]; Rogers, et. al. [48]; Kerr [49]; Turgeman-Goldschmidt [50]

which help *Law enforcement* investigate computer crime and cybercrime. Law enforcement is a critical control which belongs to outer containment as well. As Table VI shows, we explore the development of outer containment based on technical control, formal control and law enforcement.

C. The development of inner social control

Beebe and Rao [19] argued that inner containment conditions include a strong sense of conscience and a good self-concept. Dhillon et al. [24] suggests that informal controls are those measures that serve to inculcate employees into a culture of ethics, accountability, and proper conduct. Individual's norms and values, and education and training programs placed on ethical behavior and accountability. The development of inner containment delineated that early literatures focused on exploring attitude and awareness which help people to create correct computer user's legal behavior. Next, some literatures addressed the importance of self-control. Such informal controls correspond to containment theory's inner controls.

The illegal behavior studies, such as piracy, hacking and computer abuse, many literatures discussed the related issues in order to understand the detailed of computer user's illegal behavior. From 1991 to 2000, computer user's illegal behavior cases increased with the number of Internet users and Internet applications. Viruses, misuse, hacking, sabotage, and cyberpunks increased, leading to an increased focus on security as well. In this decade, interdisciplinary issues began to emerge regarding privacy, codes of ethics, definitions of computer abuse, deviant behavior, and the global society. From 2001 to 2006, software piracy, psychological analysis and hacker behavior were among the topics extensively explored. As Table VI shows, ethical related issues, self-control and illegal behavior studies were published past three decades.

D. The proposed model

The flourishing synergy between organized crime and the Internet has increased the insecurity of the digital world [8], and countering this synergy will require an interdisciplinary approach whereby researchers and practitioners bring their specialized knowledge to the task.

Containment theory argues that inner containment is able to the control of outer containment; hence, inner social control works better than outer social control in restraining deviant behavior [18]. Reckless [18] pointed out that inner social control and informal outer social control (e.g., parent and peers) maintain social orders well in conservative and traditional society. In high speed transition of cyber society, outer social control may work better than inner social control in restraining computer user's illegal behavior. To delineate the extensibility of containment theory in the digital realm, Figure 1 shows a picture of social control education, inner social control and outer social control to restrain computer user's illegal behavior intention. The basic contention of the model is that computer user's illegal behavior intention can be influenced by perceived inner social control and perceived outer social control. Not only are both social controls able to be influenced by social control education, but also increases inner social control if presents well-structured outer social control. Extension of containment theory to explain computer user's illegal behavior intention then leads to the following propositions.

Social control education is defined that educating computer user (e.g., organizations and individuals) safe and correct methods in using computers, information systems and Internet. Social control education includes two parts: (1) outer containment education, which help computer user understand the current protections served by technical control, formal control and law enforcement; (2) inner containment education, which help computer user building up correct cyber-ethics behavior. Providing social control education to computer user, which is able to help computer user to perceive both inner and outer social control. Hence, this study leads two propositions following:

Proposition 1. Social control education is positively associated with the perceived inner social control.

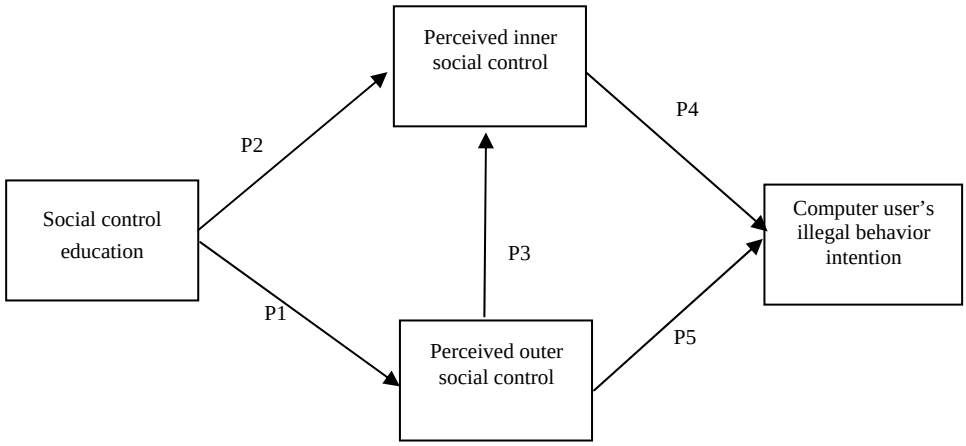

Figure 1 Proposed model for restraining computer user's illegal behavior intention

Proposition 2. Social control education is positively associated with the perceived outer social control.

Intrusion detection system, auditing and log reviews, encryption, user training and reporting policies, and vulnerability patches are methods to restrain illegal behavior. When organizations and individuals know to set up technical and formal control, and they agree to report policies in case they are attacked. When computer users perceive well-structured outer social control, which may aggregate perceived inner social control. This study leads the third propositions following:

Proposition 3. Outer social control is positively associated with the inner social control.

When computer users perceive both inner and outer social control, both containments are able to restrain computer user's illegal behavior intention. Hence, this study leads two propositions following:

Proposition 4. Perceived inner social control is positively associated with computer user's illegal behavior intention.

Proposition 5. Perceived outer social control is positively associated with computer user's illegal behavior intention.

This study proposed the importance of social control education. Social control education help organizations and computer users pay attention on both inner and outer containments. Hence, this study proposes proposition 1-2. Proposition 3 highlights the importance of outer social control. Propositions 4-5 follow directly from containment theory.

V. CONCLUSIONS

Based on the computer crime and cybercrime publications between 1968 and 2009, all publications are analyzed and evaluated to determine the quantitative characteristics of illegal behavior research studies. According to the containment theory, this study proposed a model of restraining computer user's illegal behavior intention. For organizations and individuals, privacy, knowledge and information are intangible asset of enormous value. However, there are still many challenges remain: Who will lead the social control education promotion? How to request organizations and individuals increasing their outer containment and inner containment to restrain computer user's illegal behavior?

In the short term, more support for the study of computer user's illegal behavior is urgently needed, and such support will be crucial in the long term to meeting growing cyber-society needs. While the present integrated study of academic writing on computer user's illegal behavior serves to illustrate trends in the professional literature, continuing research will be needed if we are to realize the goal of reducing and eventually preventing computer user's illegal behavior.

REFERENCES

[1] O. Grynszpan, J.C. Martin, and J. Nadel, "Multimedia interfaces for users with high functioning autism: An empirical investigation," *Journal of Human-Computer Studies*, vol. 66, pp. 628-639, 2008.

[2] J.Y. Lai, "Assessment of employees' perceptions of service quality and satisfaction with e-business," *Journal of Human-Computer Studies* vol. 64, pp. 926-938, 2006.

[3] J. Ing-Marie, N. Clifford, M.L. Kwan, "Mixing personal computer and handheld interfaces and devices: effects on perceptions and attitudes," *International Journal of Human-Computer Studies*, vol. 61, pp. 71-83, 2004.

[4] Y. Lin, W.J. Zhang, "Towards a novel interface design framework: function–behavior–state paradigm," *Journal of Human-Computer Studies* vol. 61, pp. 259-297, 2004.

[5] T. T. Moores, and J. Dhaliwal, "A Reversed Context Analysis of Software Piracy Issues in Singapore," *Information and Management*, vol. 41, pp. 1037-1042, 2004.

[6] M.O. Lwin, and J.D. Williams, "A Model Integrating the Multidimensional Developmental Theory of Privacy and Theory of Planned Behavior to Examine Fabrication of Information Online," *Marketing Letters*, vol. 14, pp. 257-272, 2003.

[7] M.K. Chang, "Predicting Unethical Behavior: A Comparison of the Theory of Reasoned Action and the Theory of Planned Behavior," *Journal of Business Ethics*, vol. 7, pp. 1825-1834, 1998.

[8] N. Kshetri, "Pattern of global cyber war and crime: A conceptual framework," *Journal of International Management*, vol. 11, pp. 541-562, 2005.

[9] M. Griffiths, "Excessive Internet use: implications for sexual behavior," *CyberPsychology & Behavior*, vol. 3, pp. 537-552, 2000.

[10] S.I. Chiu, J.Z. Lee, "Video game addiction in children and teenagers in Taiwan," *CyberPsychology & Behavior*, vol. 7, pp. 571-581, 2004.
[11] C.S. Wan, W. B. Chiou, "Why are adolescents addicted to online gaming? an interview study in Taiwan," *CyberPsychology & Behavior*, vol. 9, pp. 762-766, 2006.
[12] O. Palesh, K. Saltzman, C. Koopman, "Internet use and attitudes towards illicit Internet use behavior in a sample of Russian college students," *CyberPsychology & Behavior*, 7, pp. 553-558, 2004.
[13] R.E. Bell, "The Prosecution of Computer Crime," *Journal Financial Crime*, vol. 9, pp. 308-325, 2002.
[14] D. Thomas, B.D. Loader, *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*. New York: Taylor & Francis Group, 2000.
[15] D. Verton, FBI chief: Lack of incident reporting slows cybercrime fight. Available at: computerworld.com/ securitytopics/security/cybercrime/story/0,10801,75532,0 0.html. Accessed April 05, 2007.
[16] I.R. Guzman, M.L. Kaarst-Brown, "Organizational survival and alignment: insights into conflicting perspectives on the role of the IT professional," *ACM Proceedings of the 2004 SIGMIS*, pp. 30-34, 2004.
[17] W. C. Reckless, "A New Theory of Delinquency and Crime," Federal Probation, vol. 25, pp. 42-46, 1961.
[18] W. C. Reckless, *The Crime Problem* (4th Edition). New York: Appleton Century Crofts, 1967.
[19] N.L Beebe,., V.S. Rao, "Using situational crime prevention theory to explain the effectiveness of information systems security," *Proceedings of the 2005 software conference, Las Vegas*, 2005.
[20] A. Bandura, (1977), *Social Learning Theory*. NJ: Prentice-Hall.
[21] A. Bandura, "Self-Efficacy Mechanism in Human Agency," *American Psychologist*, vol. 37, pp. 122-147, 1982.
[22] K. Krippendorff, "Content analysis: an introduction to its methodology," Sage, CA: Beverly Hill, 1980.
[23] K. C. Laudon, C. G. Traver, *E-Commerce: Business, Technology, Society*. Boston, MA: Addison-Wesley, 2004.
[24] G. Dhillon, S. Moores, "Computer crimes: theorizing about the enemy within, *Computers and Security*," vol. 20, pp. 715-723, 2001.
[25] Chang, K.C., Lu, E.H., Su, P.C., "Design of traceable security system," *Applied mathematics and computation*, 168 (2), pp. 933-944, 2005.
[26] M.Y. Huang, "Critical information assurance challenges for modern large-scale infrastructures," *Lecture notes in computer science*, vol. 3685, 7-22, 2005.
[27] J.L. McMullan, D.C. Perrier, "Technologies of crime: The cyber-attacks on electronic gambling machines," *Canadian Journal of Criminology and Criminal Justice*, vol. 45, pp. 159-186, 2003.
[28] Willison, R., Backhouse, J, "Opportunities for computer crime: considering systems risk from a criminological perspective," *European journal of information systems*, 15 (4), pp. 403-414, 2006.
[29] G. Dhillon, S. Moores, "Computer crimes: theorizing about the enemy within," *Computers and Security*, vol. 20, pp. 715 – 723, 2001.
[30] G.H. Higgins, "Can low self-control help with the understanding of the software piracy problem?" *Deviant Behavior*, vol. 26, pp. 1-24, 2001.
[31] S. Haugen, J.R. Selin, "Identifying and controlling computer crime and employee fraud," *Industrial Management & Data Systems*, vol. 99, pp. 340-344, 1999.
[32] C.B. Foltz, T.P. Cronan, T.W. Jones, "Have you met your organization's computer usage policy?" *Industrial Management & Data Systems*, vol. 105, pp. 137-146, 2005.
[33] M. Groenhuijsen, and M. Schudelaro, "Balancing financial threats and legal interests in money-laundering policy," *Crime, Law and Social Change*, vol. 43, pp. 117-147, 2005.
[34] R.G. Burns, K.H. Whitworth, C.Y. Thompson, "Assessing Law Enforcement Preparedness to Address Internet Fraud," *Journal of Criminal Justice*, vol. 32, 477-493, 2004.
[35] S.W. Brenner, "U.S. Cybercrime Law: Defining Offenses," *Information Systems Frontiers*, vol. 6, pp. 115-132, 2004.
[36] F. Mendez, "The European Union and cybercrime: insights from comparative federalism," *Journal of European Public Policy*, vol. 12, 509-527, 2005.
[37] D.Y. Kao, S.J. Wang, F.Y. Huang, "Digitized forensic investigation at P2P copyright controversy," I*nfringement. Lecture Notes in Computer Science*, vol. 3975, pp. 644-646, 2006
[38] A. Arnes, P. Haas, G. Vigna, R.A. Kemmerer, "Digital forensic reconstruction and the virtual security testbed ViSe," *Lecture Notes in Computer Science*, vol. 4064, pp. 144-163, 2006
[39] J.S. Kim, M. Kim, B.N. Noh, "A fuzzy expert system for network forensics," *Lecture Notes in Computer Science*, vol. 3043, pp. 175-182, 2004.
[40] M.K. Rogers, K. Seigfried, "The future of computer forensics: a needs analysis survey," *Computers & Security*, vol. 23, pp. 12-16, 2004
[41] S. Harrington, "The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions," MIS Quarterly, vol. 20, pp. 257-78, 1996.
[42] W.P. Cordeiro, "Suggested Management Responses to Ethical Issues Raised by Technological Change," *Journal of Business Ethics*, vol. 16, pp. 1393-1400, 1997.
[43] K. Udas, W.L. Fuerst, D.B. Paradice, "An Investigation of Ethical Perceptions of Public Sector MIS Professionals," *Journal of Business Ethics*, vol. 15, pp. 721-734, 1996.
[44] P.S. Dowland, S.M. Furnell, H.M. Illingworth, P.L. Reynolds, "Computer crime and abuse: A survey of public attitudes and awareness," *Computers and Security*, vol. 18, pp. 715-726, 1999.
[45] Higgins, G.E., Makin, D.A., "Self-control, deviant peers, and software piracy," *Psychological Reports*, 95, pp. 921-931, 2001.
[46] T.P. Cronan, C.B. Foltz, T.W. Jones, "Piracy, computer crime, and IS misuse at the university," *Communications of the ACM*, vol. 49, pp. 84-90, 2006.
[47] M. Limayem, M. Khalifa, W.W. Chin, "Factors motivating software piracy: a longitudinal study," *IEEE Transactions on Engineering Management*, vol. 51, pp. 414- 425, 2004.
[48] M.K. Rogers, K. Seigfried, K. Tidke, "Self-reported computer criminal behavior: A psychological analysis," *Digital investigation 3S*, pp. S116-S120, 2006.
[49] O.S. Kerr, "Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes," *NYU Law Review*, vol. 78, pp. 1596-1668, 2003.
[50] O. Turgeman-Goldschmidt, "Hackers' Accounts: Hacking as a Social Entertainment," *Social Science Computer Review*, vol. 23, pp. 8-23, 2005.

Chi-Chao Lu, he is an instructor of center for general education at Overseas Chinese Institute of Technology, Taiwan. He received his MA from National Taiwan University and his ML from TungHai University. His current research interests include information society, cybercrime and cyber behavior.

Wen-Yuan Jen, Dr. Jen is an Associate Professor and Chairman of Institute of Information and Society at National United University, Taiwan. She received her MS from the Texas A&M University and her PhD from the National Central University. Her current research interests include e-Health, mobile service, electronic commerce and information society.