The Stephen Smith Center
A Center for Research in Computer Related Crime

A Concept Paper

Douglas E. Salane
Mathematics & Computer Science Department

The John Jay College of Criminal Justice
The City University of New York

January 18, 2006

Table of Contents

1. Introduction This report presents a proposal for a technically oriented research center for the study of computer related crime at John Jay College. The report describes the Center's function, outlines its initial research focus, and, most importantly, describes how the Center would support computer related crime research and thereby encourage faculty participation. The following is the basic concept.

The Stephen Smith Center develops and disseminates knowledge and technical solutions to counter criminal activity that involves modern information systems and their underlying computer and network infrastructures. The Center both conducts and supports research to this end. Center researchers utilize the work of the computer science, mathematics and other scientific research communities to solve vexing technical problems that arise in computer related crimes, especially in the collection and analysis of digital evidence.

Technical solutions alone are not sufficient to thwart the misuse and abuse of modern information systems. Protecting the users of these systems requires new legislation, policies and international agreements that take into account the capabilities, limitations and vulnerabilities of modern information infrastructures [7, 10, 17, 38, 39]. In addition, technologists often must be aware of legal considerations and information flows that arise in the investigation of a computer related crime [5]. Thus the Center promotes joint research efforts among the legal, criminal justice and technical communities. Interdisciplinary efforts allow Center sponsored research to address the needs of the criminal justice community and yield measurable results in fighting computer related crime.

Through its research activities and dissemination efforts, the Center is a source of expertise in the means to deter criminal activity that employs or exploits modern information systems and infrastructures. Center research addresses so-called "cybercrime," which can be defined as crime that targets information systems, computers and computer networks. Cybercrime, which often takes advantage of the anonymity afforded by modern information infrastructures, continues to pose significant challenges for law enforcement. The Center's focus, however, is broader than cybercrime since the challenges to law enforcement go beyond this type of computer crime. Today just about any white collar crime involves a computer and a network. In addition, such crimes usually leave a trail of digital evidence. Criminal investigations of financial crimes such as money laundering, for example, require the analysis of large data sets and investigators use statistical and data mining tools to find patterns and trends [18, 29]. Evidence in the recent Enron security fraud case included over 500,000 e-mail messages, which provided valuable information on links among individuals. Development of tools for the analysis of such forensic data sets and their use in law enforcement is an active area of research [1, 6, 14, 42]. The Center houses the latest data mining expertise as well as the computational and database capabilities needed to analyze the large scale data sets that often arise in computer related crimes.

The growth of the Internet and Web during the past ten years has dramatically altered economies and ways of life throughout the world. The widespread reliance on Internet

based information systems, however, has created new opportunities for traditional criminal activities such as extortion, fraud, social crimes and terrorism [8, 15, 25, 34]. Deterring the misuse and abuse of Internet based information systems and preventing the interruption of these vital systems are among the great challenges to governments and law enforcement in the early years of the 21st century. Due to the rapid development of both information infrastructures and applications, most law enforcement and government agencies must rely on the academic and outside technical communities for the computer expertise and computational tools that are needed to investigate crimes involving the Internet. (See, for example, [11, 20, 27].) Through its research programs and dissemination activities, the Center makes available cutting edge computing technology, the systems expertise, and analytical capabilities that are required to detect and address Internet abuse and misuse.

Thus far this report has described what a Center to address computer related crime could be like at John Jay College. The remainder of the report describes a plan for building such a Center. The report discusses Center activities that will foster research in computer related crime both at the College and beyond. It describes the value that a Center can offer to both researchers and practitioners. The report mentions several current research areas that are of critical importance to the criminal justice community and would be of interest to Center researchers. In addition, the report offers suggestions for staffing the Center, discusses the Center's relation to academic programs, examines funding possibilities for the Center, and notes the importance of fostering joint efforts with law enforcement and other organizations involved in computer crime research. By developing and making available cutting edge methods, systems and other tools needed to deter and analyze computer related crimes, the Center would move the College further toward its goal of becoming a national and international leader in research in criminal justice [13].

2. Center support for computer crime research Both researchers and practitioners who study or solve computer related crimes should be able to look to the Center for advanced computer expertise and technical resources for projects and investigations. Research in computer related crime requires an eclectic assortment of expertise and technology; the Center would attempt to bring these together. In addition, the Center would act as a focal point for the dissemination of research results and thus play a key role in making both the law enforcement and the technical research communities aware of issues and solutions.

Given the faculty and staff expertise at the College, the Center could provide the following to promote research in computer related crime.

(1) Computational and analytical expertise for cybercrime projects and investigations, especially expertise from the applied mathematics, computer science and statistics communities.

(2) Legal expertise on the impact and technical implications of legislation, court rulings and agency interpretations that affect information systems and network infrastructures.

(3) Specialized high-end computing infrastructures needed in research projects, e.g., high performance data systems, computer systems and research computer networks, along with the personnel to support research projects that require such systems.

(4) Forums for the dissemination of results and joint work with criminal justice practitioners, including web sites, conferences and eventually a referred journal.

(5) Criminal justice and forensic data collections and the on-line analysis, statistical and data mining tools needed to analyze these collections.

In many ways the research group associated with the Center would resemble an advanced computing group in a university or government national laboratory. These groups conduct research that results in methods, systems, software and analyses that are needed by researchers within their own and in other organizations. Often these groups pursue joint projects with researchers who require expertise or computational methods outside their knowledge domain. A research focus in these groups ensures that the latest methods and solutions are available to their organizations. By following a similar paradigm, the Center would develop and provide the broad range of technical expertise that is needed to address computer related crime – which takes advantage of ever-advancing digital technology.

The Center would provide specialized state-of-the-art computational capabilities needed for computer related crime research and investigations. For example, the Center would offer the high performance computing, database and other computer systems needed for data analysis. In addition, it would make available various data collections used in computer related crime research. Currently, researchers at the College have limited access to such resources. By working with the Center, a researcher would have access to resources needed for projects and at the same time have the opportunity to contribute to the Center's capability to support additional research.

3. Initial research focus and activities This section provides a sample of the research that would be of interest in the Center. During the past five years the College has developed new faculty expertise and acquired significant computational capabilities in areas of computing such as computer security, data mining, high performance computing, and networking. These new capabilities allow the Center and College to contribute to research efforts to develop (i) methods and systems to combat network based crime, (ii) effective techniques for the collection and analysis digital evidence, and (iii) advanced computer/database systems for forensic analysis and computer crime research. These three research areas are initial offerings and certainly the Center's scope of work would broaden or even become more focused as additional faculty members participate and relationships develop with criminal justice agencies and other researchers. Due to the need for improved capabilities to address computer related crime and the rampant abuse and misuse of modern information system infrastructures, both the National Institute of Justice and National Science Foundation have funding initiatives that would support work in each of the three research areas mentioned. (See, for example, [21, 23, 24].)

(i) Methods to analyze and combat network based crime

Crimes employing computer networks include denial-of-service, identity theft, phishing, spam, spyware, and propagation of Trojans and viruses. (The Australian High Tech Crime Center http://www.ahtcc.gov.au/glossary.aspx provides an overview.) Of particular concern are large networks of illegally commandeered computers (so-called Botnets) that frequently are used to execute these crimes on a massive scale [33]. Combating such network based crime requires new systems, methods, tools, legislation and policies. Center researchers would conduct work that impacts each of these areas. In addition, the Center could facilitate such work by providing research computer and network facilities, systems and analytical expertise, and expertise in the legal issues surrounding these crimes. For example, the Center could make available network data collections that frequently are used for work in forensic analysis of system break-ins, evaluation of intrusion detection systems, and development of network forensic analysis tools. Data collections include the MIT/DARPA corpus and a corpus of forensic data derived from the U.S. Department of Defense's Global Grid Evaluation Facility [16]. Center legal experts would help technologists understand legislation and government agency interpretations of legislation involving information infrastructures so technical solutions take into account appropriate legal requirements. Center researcher would also be concerned with quantifying the extent of these network exploits and detecting new forms.

Developing forensic capabilities in computer and communication networks is fundamental to combating network based computer crimes but presents considerable technical, organizational and legal challenges [9, 31]. Protection of privacy rights must be a central concern in the development of such systems [2]. Center research certainly would focus initially on the development of effective methods and systems for the collection and analysis of network traffic. For example, essential are efficient, reliable attack detection systems that can differentiate between attack and normal network traffic. Effective systems cannot rely on heuristics, human intervention nor the availability of extensive training data as is the case with current signature and anomaly detection systems. Promising new approaches employ signal detection methods that are based on general mathematical and statistical models of normal network traffic. The papers [12, 19 & 32] provide examples of this approach and also discuss the challenges. A second critical and difficult problem is the need to keep track of traffic passing through a network during a given period. Several faculty members in the Mathematics and Computer Science Department and a faculty member from the Law and Police Science Department already are working on an NSF funded project with researchers at Polytechnic University to develop a distributed network forensic system [30]. Finally, methods, systems and Internet management policies are needed that allow investigators and network administrators to determine quickly the source of attacks [17, 39, 41].

(ii) Analysis of digital forensic evidence

Law enforcement relies on well developed commercial systems and established practices for the collection, preservation, and analysis of forensic data found on digital devices such as computer hard drives [22, 34]. Manufacturers continue to develop these systems to provide required capabilities, for example, collection and analysis of data in a distributed environment and on devices such as cell phones, personal digital assistants and new storage devices. In addition, commercial systems increasingly must address encryption and anti-forensic techniques that make data collection and analysis difficult if not impossible. Center researchers would track developments in this area. Working with practitioners and other researchers, they would investigate the capabilities and limitations of the latest commercial systems.

Center research will take advantage of methods currently being developed by the knowledge discovery community for detecting unknown patterns and trends in large data collections. Often referred to as data mining or knowledge discovery techniques, the methods include information retrieval, cluster analysis, social network analysis and other techniques that have their foundations in the fields of artificial intelligence, graph theory, information theory and statistics. An overview of data mining techniques and recent applications in crime analysis can be found in [4, 18, 36, 37, 40]. Knowledge discovery methods have generated considerable interest in scientific fields where large data sets need to be analyzed. A number of research institutions are building capabilities in knowledge discovery with a focus on scientific applications. (See, for example, [26]). Although data mining techniques have been used to detect money laundering, credit card fraud and other financial crimes, their use in law enforcement is limited largely to elite investigative units in federal agencies that have adequate budgets for highly trained personnel and specialized consulting services. As law enforcement increasingly is called upon to investigate crimes involving modern information systems, the tools of the knowledge discovery community will be essential for forensic analysis and must be more widely available. Center researchers will both develop such tools and investigate their use and limitations in investigations. In addition, the Center could be a valuable source of information for both law enforcement practitioners and other computer crime researchers. The Mathematics and Computer Science Department now has the requisite expertise in artificial intelligence, statistics and other areas of computing needed to pursue work in this area. The Department continues to seek new faculty members with an interest in data mining and related areas.

(iii) Advanced computer systems for forensic analysis and computer crime research

If the Center is to participate in the development of methods and systems to fight computer related crime, Center researchers and others supported by the Center will require access to specialized computing systems and software, advanced computing expertise, and database systems that provide both simple query and on-line analysis capabilities. Currently researchers at the College have limited access to such systems, expertise or exploratory data capabilities. The Center would seek funding to maintain required specialized computing facilities and support highly trained personnel who would not only maintain advanced systems but also develop detailed knowledge of the high performance computing systems, specialized software and analytical methods needed to

support research projects. Faculty members interested in working with the Center have already attracted some funding for the required computational facilities from NASA and NSF. Under the auspices of a recent NASA award, the Mathematics and Computer Science Department built research computer facilities for work in networking and high performance computing [28].

Center computing facilities and advanced computing expertise would be the nexus of the Center. These would attract researchers who require advanced computational capabilities but who individually have neither the expertise nor resources to build and maintain such capabilities. The construction of center computer systems would be research projects in themselves and would provide models for groups involved in the design of data systems for homeland security applications and systems for studying criminal justice data [3]. The availability of high performance computing platforms, on-line data analysis capabilities, research computer networks, and specialized systems for intrusion detection studies would encourage collaborations between Center researchers, researchers on and off campus, and practitioners. Indeed, Center facilities would make it worthwhile for researchers to become involved in Center activities and contribute to Center capabilities for research in computer related crime.

4. Center researchers and support staff Personnel associated with the Center would include members of the John Jay faculty; researchers at other institutions including security firms, forensic laboratories and other universities; and a small and highly trained support staff. Researchers associated with the center would benefit from Center dissemination activities, a continuous flow of challenging problems, and access to the computing systems, support staff and other technical expertise needed for their research. Also encouraging researchers to participate would be the prospect of collaborative efforts with practitioners who require access to state-of-the-art methods and research.

The Center must maintain a small but highly trained support staff, an essential requirement for computer related crime research that requires access to extensive expertise in the systems areas of computing. This staff could be assisted by graduate students and even qualified undergraduates as part of internship programs. Access to such a staff would be an incentive for researchers to participate in Center activities and contribute to the Center. Eventually, the Center would require administrative support to manage grant funded activities and help prepare proposals.

The success of the Center depends on attracting an enthusiastic core of faculty members who are active researchers in the area of computer related crime. The core faculty members would procure external funding to support Center activities; oversee operations of the Center; and carry out basic research in computer science, criminal justice, legal research, and statistics that would impact many areas of computer related crime research. Incentives for core faculty participation include the following: (1) numerous joint collaborations, (2) access to Center resources, (3) ability to attract larger funding amounts, and (4) the opportunity to shape the Center and influence its directions.

5. Relation to academic mission The Center can contribute to and benefit from the academic programs of the College. For example, the Forensic Computing Graduate program has students with the basic computing background needed to work on Center projects. These students could use Center equipment, when it is not needed for research activities, to develop advanced skills and specialized expertise that would allow them to participate in research projects. Thus the Center and academic programs, both in computing and other areas, would benefit from a synergistic interaction. The Center's recent contribution of excess equipment to the Forensic Computing Graduate Laboratory is another example of the way the Center can assist an academic program. A number of federal programs, e.g., NSF Research at Undergraduate Institutions, NASA's Project Ascend McNair Program, and Department of Education's Minority Science Improvement Program fund efforts that encourage both undergraduate and graduates to become involved in research. Moreover, by developing relations with academic programs, the Center would interest students in research and encourage them to pursue advanced degrees thereby contributing to the academic vitality of the College.

6. Funding and College support External funding to support Center activities and its research programs is essential. Center activities and research will require advanced computer facilities, highly trained support staff, and a significant commitment on the part of the involved faculty members. College support and currently available funds will allow the Center to begin operations on a relatively small scale, but building a Center that functions as described in this proposal will only be possible with significant external funding. College support, however, always will play a role and will be essential in the initial stages.

To attract funding the Center must be an active organization with programs, facilities and support staff. The Center must have in place research programs that are producing measurable results. Funding agencies must see evidence that those submitting proposals have access to the support personnel, computing facilities, data collections and the computing expertise needed to carry out research in computer related crime. A significant commitment on the part of the College must be evident as well. Furthermore, a key consideration in many funding decisions is that the work is done as part of a group where it can be leveraged by other researchers, which is a good reason for a researcher to work with the Center. The Center could begin some proposed activities and research by (1) utilizing funds currently available to the Center, (2) taking advantage of institutional capabilities in the Mathematics & Computer Science Department developed under previous NASA and current NSF funded grants, and (3) supporting current faculty research efforts in computer networking, data mining and legal research that impact computer related crime research.

7. Joint work with law enforcement and other research organizations Center researchers must establish relationships with practitioners in law enforcement, and with computer crime and computer security researchers in federal crime labs, security firms, universities and government laboratories. Relationships with practitioners will ensure a flow of practical problems into the Center and allow Center research to be applied to these problems. Relationships and collaborations with the research communities will enable Center researchers to be aware of the latest research developments and methods available to fight computer related crime. By involving both researchers and practitioners, the Center certainly can facilitate dissemination of results and knowledge needed to address computer related crime.

The Center must take advantage of the College's existing relationships with law enforcement agencies and continue to build relationships with both government and university research organizations involved in computer security and computer related crime research. Faculty members interested in the Center already have working relationships with members of the Secret Service New York Electronic Crimes Task Force and the NYPD Computer Crime squad. In addition, interested faculty members already are participating in several externally funded research projects in computer security and forensics with researchers at other universities. The success of the Center will require that relationships with both law enforcement and the research communities be expanded and lead to joint projects that utilize Center expertise and research. By being fully engaged in the current research environment, the Center can play a valuable role in bridging the gap between researcher and practitioner.

8. Conclusion The Stephen Smith Center will promote and conduct research that leads to methods, systems, new policies and legislation to deter computer related crime. Center resources, expertise and activities will support both researchers and practitioners who require cutting edge methods, systems and technologies to counter crime that takes advantage of ever-advancing digital technology. Through its research and dissemination efforts, the Center will make available the knowledge and tools needed to address criminal activity in the Internet age.

9. References

1. Adibi, J. & Shetty, J. (2005). Discovering important nodes through graph entropy: The case of Enron email database, In proceedings *Third International Workshop on Link Discovery*, Chicago, IL, August 21, (pp.74-81). New York: ACM Press.

2. Bayardo, R.J. & Ramakrishnan, S. (2003, September). S. Technological Solutions for Protecting Privacy. *Computer*, 36 (9), 115-118.

3. Carey, D.W. (2003, May). Information assurance post 9-11: enabling homeland security. *Cross Talk: The Journal of Defensive Software Engineering.* Retrieved August 10, 2005 from http://www.stsc.hill.af.mil/crosstalk/2003/05/carey.html.

4. Chen, H., Chung, W., Xu, J., Wang, G., Qin, Y. & Chau, M. (2004, April). Crime data mining: a general framework and some examples. *Computer*, 37 (4), 50-57.

5. Ciardhuán, S. Ó. (2004, September). An extended model of cybercrime investigations. *International Journal of Digital Evidence*, 3 (1), 1-22. Retrieved October 9, 2004 from http://www.ijde.org/archives_home.html.

6. Cohen, W. (2005, April 4). The Enron Email dataset. Retrieved October 10, 2005 from http://www.cs.cmu.edu/~enron/.

7. Colombell, M.R. (2002, Spring). The legislative response to the evolution of computer viruses. *The Richmond Journal of Law and Technology*, 8 (3). Retrieved March 2005 from http://law.richmond.edu/jolt/v8i3/article18.html.

8. Donahue, T. (2005, June 23). Information technology facing security crossroad. Talk presented at the United States Secret Service's New York Electronic Crimes Task Force Quarterly Meeting, New York, NY. A CIA analyst describes the vulnerabilities that arise when Internet-based systems are used to control physical infrastructures.

9. Escudero-Pascual, A. & Hosein, A. (2004, March). Questioning lawful access to traffic data. *Communications of the ACM*, 47 (3), 77-82.

10. Gross, G. (2005, December 20). FTC: Computer Users Seeing Less Spam, Law Helped. NetworkWorld, IDG News Service, December 20, 2005. Retrieved December 27, 2005 from http://www.networkworld.com/news/2005/122005-ftc-spam.html?page=1.

11. Harrison, W., Heuston, G., Mocas, S., Morrissey, M. & Richardson, J. (2004, July). High-Tech Forensics. *Communications of the ACM*, 47(7), 48-52.

12. Hussain, A., Heidmann, C. & Papadopoulous, C. (2004, June 2). Identification of repeated attacks using network traffic forensics. (Report No. ISI-TR-2003-577b). Information Sciences Institute, University of Southern California, Los Angles, CA.

13. John Jay College of Criminal Justice. (2005, April 1). Monitoring report: strategic plan outcomes assessment plan facilities plan. New York, NY.

14. Keila, P.S. & Skillicorn, D.B. (2005, June). Detecting unusual and deceptive communiation in email. School of Computing, Queens University, Kingston, Ontario. Retrieved September 10, 2005 from http://www.cs.queensu.ca/TechReports/Reports/2005-498.pdf

15. Leyden, J. (2003, November 12). East European gangs in online protection racket: Blackmail by DDoS. *The Register*. Retrieved November 20, 2005 from http://www.theregister.co.uk/2003/11/12/east_european_gangs_in_online/**.**

16. Lincoln Laboratory – MIT. (1999). Darpa intrusion detection evaluation data set overview. Lexington, MA. Retrieved March 7, 2005 from http://www.ll.mit.edu/IST/ideval/data/1999/1999_data_index.html.

17. Lipson, H.F. (2002, November). Tracking and tracing cyber-attacks: Technical challenges and global policy issues. (Report CMU/SEI-2002-SR-009). CERT Coordination Center, Carnegie Mellon Software Engineering Institute, Pittsburgh, PA.

18. Mena, J. (2003). *Investigative data mining for security and criminal detection*. New York, NY: Butterworth Heinemann.

19. Mukkamala, S. & Sung, A.H. (2003, Winter). Identifying significant features for network forensic analysis using artificial intelligence techniques. *Journal of Digital Evidence*, 1(4) 1-17.

20. National Association of Attorney Generals. (2005). Projects: Cybercrime. Available at http://www.naag.org/issues/issue-cybercrime.php.

21. National Institute of Justice. (2005, October). Solicitation for Concept Papers: Electronic Crime Research and Development. Washington, D.C. Retrieved November 29 from http://www.ncjrs.org/pdffiles1/nij/sl000722.pdf.

22. National Institute of Standards and Technology. (2005, August). Guide to computer and network data analysis: applying forensic techniques to incident response. (SP 800-86). Gaithersburg, MD: Grace,T., Chevalier, S., Kent, K. & Dang, H. Retrieved September 10, 2005 from http://csrc.nist.gov/publications/drafts/Draft-SP800-86.pdf

23. National Science Foundation. (2005). Cyber Trust (CT). (Program Solicitation 06-517). Retrieved December. 20, 2005 from http://www.nsf.gov/pubs/2006/nsf06517/nsf06517.pdf.

24. National Science Foundation. (2005). Networking Technology and Systems (NeTS). (Program Solicitation 06-516.) Retrieved December 20, 2005 from http://www.nsf.gov/pubs/2006/nsf06516/nsf06516.pdf.

25. Poulsen, K. (2004, August 26). FBI busts alleged DDoS Mafia. *SecurityFocus.* Retrieved March 2005 from http://www.securityfocus.com/news/9411.

26. Purdue University. (2003, May 15). Massive Data: Management, Analysis, Visualization, and Security: A School Focus Area. Retrieved October 10, 2005 from http://www.science.purdue.edu/about_us/strategic_plan/COALESCEAreas/MassiveData 03may.pdf.

27. Purdue, Law Enforcement Probe Digital World of Computer Forensics. (2004, August 13). *Science Daily*. Retrieved December 28, 2005 from http://www.sciencedaily.com/releases/2004/08/040812052256.htm.

28. Salane, D. and Bondarenko B. (2004, July). Cluster Computing in a College of Criminal Justice. Talk presented at Usenix '04 Annual Technical Conference, Boston, MA, June 2004. Slides available at http://www.usenix.org/events/usenix04/tech/sigs/salane.pdf.
Paper available at http://web.math.jjay.cuny.edu/reports/USENIXTechnicalConference2004.pdf.

29. Senator, T.E., Goldberg, H.G., Wooton, J., Cottini, M.A., Khan, A.F., Klinger, C.D., Llamas, W.M., Marrone, M.P. and Wong, R.W. (1995). The Financial Crimes Enforcement Network AI System (FAIS) Identifying Potential Money Laundering from Reports of Large Cash Transactions. *AI magazine*, 16 (winter), 21-39.

30. K. Shanmungasundaram, N. Memon, A. Savant, and H. Bronnimann. (2003). *Fornet: A Distributed Forensics Network.* Presented at The Second International Workshop on Mathematical Methods, Models and Architectures for Computer Networks, St. Petersburg, Russia. Paper retrieved January 15, 2004 from http://isis.poly.edu/projects/fornet/.

31. Shim, S., Gong, L., Rubin, A.D. and Gwenmap, L. (2004, June). Securing the High-Speed Internet. *Computer*, 37(6), 22-32.

32. 2Stolfo, S., Lee, W., Chan, P.K., Fan, W. and Eskin, E. (2001, September 9). Data Mining-based Intrusion Detectors: An Overview of the Columbia IDS Project. *SIGMOD*, 30(4), 5-14.

33. U.S. Department of Justice. (2005, November 3). Computer virus broker arrested for selling armies of infected computers to hackers and spammers. Retrieved November 20, 2005 from http://www.usdoj.gov/criminal/cybercrime/anchetaArrest.htm.

34. U.S. Department of Justice. (2002, July). Searching and seizing computers and obtaining electronic evidence in criminal investigations. Retrieved November 20, 2005 from http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm.

35. U.S. Department of Justice. (2005, November 17). Six defendants plead guilty in Internet identity theft and credit card fraud conspiracy. Retrieved November 20, 2005 from http://www.usdoj.gov/criminal/cybercrime/mantovaniPlea.htm.

36. Vel, O., Anderson, A., Corney, M. and Mohay, G. (2001, December). Mining E-mail content for author identification forensics. *SIGMOD*, 30, 55-64.

37. Wang, G., Chen, H. and Atabakhsh, H. (2004, March). Automatically detecting deceptive criminal identities. *Communications of the ACM*, 47(3), 70-76.

38. Warkentin, M., Luo, X. and Templeton, G. F. (2005, August). A framework for spyware assessment. *Communications of the ACM*, 48(8), 79-84.

39. World Summit on the Information Society. Report from the working group on Internet governance, Report No. WSIS-II/PC-3/DOC/5-E, August 3, 2005. Available at http://www.itu.int/wsis/docs2/pc3/html/off5/index.html.

40. Xu, J.J. and Chen, H. (April 2005). CrimeNet Explorer: A Framework for criminal network knowledge discovery. *ACM Transactions on Information Systems*, 23, 201-226.

41.Yasinac, A. and Manzano, Y. (2001). Polices to enhance computer and network forensics. *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*, Westpoint, NY, June 5-6, (289-295), Los Alamitos: IEEE Press.

42. Zhang, Z., Salerno, J. and Yu, P. (2003). Applying datamining in investigating money laundering crimes. *Proceedings of the Ninth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, New York, NY, (747-752), New York: ACM Press.