Transnational Crime and Corruption Center
2000 Annual Conference
Conference Report

Transnational Crime, Corruption, and Information Technology

November 30-December 1 2000

Sponsored by the Hills Family Foundation and the Transnational Crime and Corruption Center

Conference Co-chairs
Dr. Louise I. Shelley and John T. Picarelli, TraCCC

Foreword

On behalf of the Transnational Crime and Corruption Center (TraCCC) at American University, it is our pleasure to provide you the report from our 2000 Annual Conference on Transnational Crime, Corruption and Information Technology.

We were very excited at the dynamic set of speakers and the knowledgeable and international audience we attracted to this meeting from the diverse communities we seek to reach: policymakers, scholars, law enforcement, government, business, NGOs, the public and the media. The thought-provoking panels and ensuing dialogue demonstrated the spectrum of issues that the confluence of transnational crime, corruption, and information technology generate.

Our meeting provided an international, multi-disciplinary forum that addressed the complex issues relating to the control of information technology from abuse by criminals and corrupt individuals without losing the economic and democratizing benefits of this new technology.

The drive to regulate and protect information technology has been done without understanding the full dimensions of the organized crime and corruption phenomena. The panels assessed the diverse dimensions of the transnational crime and corruption problem using actual case materials and the experiences of government and business.

We brought TraCCC's unique international perspective to bear in addressing the diverse nature of the problem and response from different regions of the world. Our focus was not only on analysis but also on developing international creative strategies through partnerships that will address transnational crime and corruption undermining the potential of information technology. We are committed to continuing exploration of ways that new technology can be used to address transnational crime and corruption without jeopardizing fundamental civil rights.

TraCCC feels that this meeting served as the foundation for our research, training and a policy agenda that will address the emerging field of transnational crime, corruption and information technology. We look forward to continuing work on these issues in the future.

Acknowledgements

We express our deep appreciation to the Hills Family Foundation for making this conference possible. We would also like to recognize Conference Manager Erica Blodgett for her tireless efforts overseeing the planning and other logistics issues associated with the conference. Third, we thank all the members of TraCCC that volunteered their time and energy preparing for the conference. Finally, we would be remiss if we did not thank the speakers for their thought-provoking presentations delivered at the conference.

Transnational Crime, Corruption, and Information Technology

Published by the
Transnational Crime and Corruption Center
240 Nebraska Hall
American University
4400 Massachusetts Avenue, NW
Washington, DC 20016-8178
Tel. 202-885-2657
Fax 202-885-1389
E-mail: traccc@american.edu
http://www.american.edu/traccc

Table of Contents

Agenda

Day 1 November 30th

Opening Speakers

- Dr. Benjamin Ladner
  President, American University
- Louise Shelley
  Director, TraCCC

Panel I Survey of Information Technology in Crime and Corruption

MODERATOR: John T. Picarelli
Analyst, TraCCC

SPEAKERS and TOPICS:

- Trafficking in Human Beings and Child Pornography
  - Alexis Slebodnick
    Senior Intelligence Analyst, US Customs Cybersmuggling Center
- Counterfeiting, Fraud, and Identity Theft
  - Mark Childers
    Special Agent, US Secret Service Electronic Crimes Branch
- Use of Telecommunications in the Commission of Crimes and Mitigation Tactics
  - John Beasley, Jr.
    Assistant US Attorney, US Department of Justice Transnational/Major Crimes Section
- Piracy of Intellectual Property
  - Timothy Trainer
    President, International AntiCounterfeiting Coalition, Inc.
- The Corporate Response to Criminal Usage of Technology Products
  - Vic Winkler
    Principal Architect-Security, Sun Microsystems Federal, McLean, VA

Lunch Keynote Speaker

- Michael Vatis
  Director, National Infrastructure Protection Center, FBI

Panel II International Perspective

MODERATOR: Vladimir Brovkin
Senior Fellow, TraCCC

SPEAKERS and TOPICS:

- The View from the Former Soviet Union
  - Mikhail Vertuzaiev
    Professor and Senior Research Fellow, National Academy of Interior Affairs of Ukraine
- The View from Asia
  - Dinkar Gupta
    Deputy Inspector General, Intelligence Division, Punjab Police, India
- Corruption
  - Michael Hershman
    Chairman, Decision Strategies/Fairfax International, LLC

Panel III Encryption and Privacy

MODERATOR: Walter D. Broadnax

Dean, School of Public Affairs, American University

SPEAKERS and TOPICS:

- Use of Technology to Mask Criminal Activity
  - Dr. Dorothy Denning
    Director, Georgetown Institute for Information Assurance, University of Georgetown
- Private Sector View
  - Jay Wack
    Chief Technology Officer, TECSEC Incorporated
- Effects of Regulation
  - Jim Kerins III
    President, National Fraud Center

Panel IV Digital Networks

MODERATOR: Dr. Nanette Levinson
Associate Dean and Associate Professor, School of International Service (SIS), American University

SPEAKERS and TOPICS:

- The Digital Networking of Malevolent Non-state Groups
  - Matthew Devost
    Senior Information Security Analyst, Security Design International Inc.
- Monitoring of Digital Networks
  - Marc Zwillinger
    Partner, Kirkland and Ellis
- The Effects of Digital Networking and Network Monitoring on Democracy
  - Mike Godwin
    Policy Fellow, Center for Democracy and Technology
- The View from the Legislative Branch
  - Makan Delrahim
    US Senate Judiciary Committee Staff

Day 2 December 1st

Panel V Finding Creative Solutions

MODERATOR: Louis Goodman
Dean, SIS

SPEAKERS and TOPICS:

- Intelligence Analysis for Cyberthreats
  - Phil Williams and Casey Dunleavy
    Computer Emergency Response Team
- The Importance of Public–Private Partnerships
  - John Tritak
    Director, Critical Infrastructure Assurance Office
- Global Forum on Fighting Corruption
  - Captain Michael Orfini, USN
    Military Advisor for National Security Affairs to the Vice President

Panel VI Identifying and Facing New Challenges

MODERATOR: Louise Shelley
Director, TraCCC

SPEAKERS and TOPICS:

- Corporate Response and Regulation
  - Mary Riley

Director, Digital Risk Management, Price-Waterhouse Coopers

- Challenges to Novel Computer and Communications Technologies
  - David von Vistauxx
    Trelex Associates, Ltd.
- Law Enforcement Operations and Challenges
  - Lou Degni
    Special Agent, Drug Enforcement Administration
- E-Readiness
  - Helena Plater-Zyberk
    McConnell International

Preface

Louise Shelley's opening remarks, detailing the purpose of the conference, noted that prior analysis has segmented transnational crime and information technology as separate entities. The conference thus sought to address the following themes:

- Integration of the requirements of the technology and business communities, government regulators, policymakers, NGOs, and foreign governments to bring diverse communities together
- Location of the proper balance between the need to regulate information technology with the desire to control the negative effects of transnational crime
- Maximization of technology's contributions to economic growth and democratization and minimization of the potential for criminal activity
- Identification of the disparate capacities of countries to work against crime committed through information technology
- Recognition of the notion of national sovereignty in producing regulatory solutions for global digital networks
- Construction of networks to address criminal networks' use of information technology

The following categories represent some of the more pertinent facts that support arguments made regarding these themes.

International Perspectives on Criminal Use of Information Technology

- Information technology links developing and developed regions rapidly
- Information technology globalizes corruption through the transfer of illicit gains
- India
  - Information technology professionals, such as engineers and software experts, known to commit crimes
  - Software piracy is a major problem, with over 90% of software pirated
  - Use of cell phones by criminals and terrorists from prison another problem
  - Shortage of trained personnel in law enforcement with information technology knowledge
  - Beginning to use public-private partnerships to address problem
- Ukraine
  - Ukrainian criminals heavily involved in Internet fraud, Ukrainian law enforcement not capable of addressing
  - Partnerships between banks and law enforcement do not exist to address abuse of bank cards
  - Ukrainian information technology specialists also known to commit and facilitate crimes

Why Information Technology is Central to the Commission of Crime

- Anonymity increases the difficulty of decoding encrypted messages
- Provides safe, secure and rapid communication
- Assists document fraud
- Internet facilitates piracy and counterfeiting of goods
- Internet facilitates terrorism through recruitment, fund raising, communications
- Basis for more robust communication systems, such as cell phones, telex, and virtual private

networks
- Aids transport, as criminals can monitor and divert shipments
- Facilitates covert banking through such means as electronic funds transfers, debit cards, and credit cards
- Provides unsophisticated criminals access to sophisticated tools

Problems of International Cooperation

- Many foreign counterparts lack computer access or knowledge
- The global information infrastructure is outside the jurisdiction of any one country
- Different legal codes and procedures impede cooperation
- Many countries lack laws to address computer crime and crimes committed by means of other forms of information technology

Balancing Civil Liberties and the Need to Regulate Information Technology

- Maintenance of privacy and confidentiality
- Insurance of the security and integrity of digital signatures
- Problems of individuals having access to private medical information and others through porous systems
- Enactment of Privacy/Computer Secrecy Act—responsibility to protect privacy of data in the US
- European Protection Act provides significant data for law enforcement while shielding it from business
- Privacy advocates support need to ensure private, legitimate communications and want limits on law enforcement's access to encryption keys
- US laws forcing paperwork into the electronic environment while safeguarding privacy in the non-paper environment is more difficult
- Network monitoring by private entities is possible under Title III
- Different requirements for monitoring by private and government entities
- Reasonable right to privacy on Internet raises questions when terrorists and criminals exploit these technologies for their use

Future Trends

- Disruption of public integrity
- Disruption of financial markets
- Corporate espionage through denial of service or the positing of false information from foreign sources
- Serious intrusions into critical systems—an "Exxon Valdez" waiting to happen

Tools to Respond

- Public-private partnerships, such as government and ISP cooperation against child pornography
- Citizen assistance in identifying potentially problematic websites
- Coalition vulnerability assessment teams
- Active security research community
- Network monitoring by private corporations

Introduction: Purpose of the Conference

The information revolution has brought both positive and negative changes to business, international affairs and daily life. New information technology is being exploited, and trends in information technology development are affecting both transnational criminal activity and crime prevention.

The conference examined challenges to the growth of information technology and its democratizing impact. We addressed the negative impact of and reactions to these new technologies in terms of the role of the state, the issue of regulation, and the challenge of balancing both public and private interests against the potential misuse of the new technology. Some of the issues the conference addressed include:

- How is the role of information technology being undermined by transnational crime and corruption?
- How are trends in information technology development affecting transnational criminal activity and crime prevention?
- How might transnational crime and corruption affect current and new technologies, firms, and institutions?
- Would new or modified regulation play a role in curtailing activity, or would the harms outweigh the benefits?
- Will regulation to control transnational crime and corruption undermine democratization and economic growth?

The conference drew upon TraCCC's successful model of multidisciplinary and multinational research initiatives to assemble constructive and thought-provoking panel discussions. The conference also served as the basis for future research and training materials for TraCCC and the Schools of International Service and Public Affairs at American University in the emerging fields of transnational crime and corruption. What follows are summations of the themes from each panel and the remarks that each presenter provided. After conducting this for each of the six panels and the presentation of our keynote address, the conclusion will return to the introductory questions to identify what the conference was able to accomplish and what research or questions remain.

Panel I Information Technology in Crime and Corruption

The opening panel of the conference set the context within which the panels that followed would examine their respective issues.[1] The panelists, all government or private sector experts on various types of criminal activity that exploit technology, noted that the rapid growth of technology, especially the seemingly limitless growth of the internet, is changing the ways that criminals and law enforcement operate. From their talks, it is possible to identify four significant observations on how criminal activities utilize technology and the ways that their organizations are responding to these challenges.

The enhancement of anonymity that today's information technologies offer was the first observation that many of the panelists touched on. Technologies such as e-mail, Internet Relay Chat, chat rooms, newsgroups, encryption, and online anonymizing services are often cited as providing criminals new ways to operate illicit enterprises. For instance, criminal syndicates

[1] By prior agreement, the first panel was closed and the panelists provided their remarks in a not-for-attribution setting. Hence, the summary of the first panel does not mention the remarks of each panelist, but rather draws out the key themes addressed during the panel.

have started employing anonymizing email services in the conduct of different types of criminal activities. One example of this trend is the use of computers by Nigerian criminal groups to mass e-mail scam letters to persons around the globe—a new variation of more traditional scam letters that once flowed from fax machines. While it is difficult to identify which criminal enterprise has benefited most from these technologies, the panelists singled out how technology has had a profound impact on the production of child pornography and the ways corruption is undertaken as illustrations of how technology has impacted criminal enterprises.

A second observation that the panelists noted was the ways that technology enhances the ability of organized crime to conduct its businesses. Focusing more broadly than the anonymizing effects of technologies, speakers made two key points in this regard. First was noted that the pace of technology improvements is vastly outstripping the abilities of law enforcement to keep pace in terms of analyzing how criminals might exploit new technologies and how law enforcement might employ novel technologies in their investigations of organized crime. The other key point was that criminals have found ways to employ technology to commit traditional forms of crime in enhanced or novel ways. An example of the latter, one speaker noted, is the piracy of intellectual property that is plaguing the entertainment industry worldwide. Through the use of powerful computers and the Internet, major criminal organizations are funding themselves through the global production, sale, and distribution of copyrighted materials.

The third observation was that, while major advancements in technology are bringing people together worldwide, technology brings together those seeking to engage in illicit activity and thus assists in the construction of criminal enterprises. One place where this is most clear is in the production of child pornography, where "support networks" of pedophiles have emerged that use the Internet and other communications technologies to encourage the production and distribution of child pornography. Another example was the ability to create a more consolidated global market for pirated intellectual property, such as software, using the Internet as a backbone. Hence, one must note that criminal elements benefited from the communications revolution that the information technology revolution has supported.

Finally, the speakers discussed the uneven technical capabilities that one finds across the spectrum of international law enforcement. Some speakers noted the difficulties in starting and managing a case that involves foreign jurisdictions, such as for international piracy of intellectual property, due to insufficient or non-existent legal measures to address the crime. Others noted that the capabilities of law enforcement to investigate and conduct organized crime cases that involve a technology element vary widely across borders. Finally, turning to the situation in the US, the speakers noted some additional difficulties, such as in explaining the use of advanced technologies in layman's terms for judges and juries during a trial. While this is likely to change as technology diffuses throughout society, the inner workings of technology are often a mystery to those that serve in these important capacities, and thus the panelists urged investigators and prosecutors to keep this in mind when undertaking such cases.

Turning to responses and capabilities, the panelists outlined diverse initiatives to counteract a wide variety of technology-driven or dependent organized criminal activities. One such capability that the panelists introduced was the Cybersmuggling Center of the US Customs Service. Located in northern Virginia, the US Customs Service founded the center in 1997 to address child exploitation, other forms of cybercrimes, and the development of computer forensics. Staffed with nearly 20 agents, the center enforces the 400-odd laws that the Customs service addresses. While the Customs Service focuses on controlling the borders of the US, the Cybersmuggling Center addresses criminal activities that virtually cross the "functional equivalent of the border." The center places a strong emphasis on collaborative relationships—

the child exploitation unit, for example, has forged strong working relationships with foreign and domestic law enforcement agencies as well as the National Center for Missing and Exploited Children (a prominent US public-private venture). In the end, while cases often present novel challenges in terms of jurisdiction and forensics, the Cybersmuggling Center is forging new ground in surmounting these obstacles.

Keynote Address

Michael Vatis, the Director of the FBI's National Infrastructure Protection Center (NIPC), provided the keynote address for the conference. The NIPC, which brings together representatives from US government agencies, state and local governments, and the private sector, serves as the US government's focal point for threat assessment, warning, investigation, and response for threats or attacks against our critical infrastructures—such as telecommunications, energy, banking and finance, water systems, government operations, and emergency services. Director Vatis introduced the purpose and capabilities of his organization in addressing the range of challenges faced by our national infrastructure.

Opening his talk, Director Vatis noted that a primary challenge in this information age is that the Internet allows people that harm networks to do so remotely and anonymously. There are thousands of websites that individuals can use to download automated tools that can make even the most non-technologically oriented person into expert hackers; thus the tools for exploiting technology in a harmful fashion are widely distributed.

Furthermore, one no longer speaks of information infrastructures in terms of national scope, but rather we recognize that an integrated global information infrastructure exists. Infrastructures are those services that are critical to the national defense or economy, such that if hackers destroyed one or debilitated its functioning significantly, it would lead to a significant impact on economic or other well-being. Electrical energy and telecommunications are particularly important in this regard because they underlie all other infrastructure sectors. Thus, the potential for harm is widespread, covering numerous potential targets and vulnerabilities.

However, this is matched with a broad spectrum of potential bad actors. In the past, it was easier to place suspects and perpetrators into classes since they were categorized into concrete crime categories. However, the present cyber threat is far more difficult to categorize because it is not easy to distinguish among the different forms of threat, which tend to resemble one another in their earlier stages. Furthermore, insiders or disgruntled employees within corporations can harm infrastructures, or foreign military organizations using combat techniques can inflict damage. A full spectrum of threats lies between these two ends.

In conclusion these threats, more often than not, turn out to be international actors and thus adds another dimension of complexity to the problem, for reasons identified in the first panel, such as coordination across multiple jurisdictions.

Panel II International Perspective

The second panel of the conference tackled the international aspects of the use of technology by transnational criminals and corrupt individuals. The conference organizers asked the panelists to address the themes presented during the first panel but from an international perspective. As the following summations demonstrate, the speakers provided detailed comments on the situation in other countries.

Michael Hershman opened up the panel by stating that he has witnessed a minimal impact on the aiding and abetting of corruption through technology, but that corruption remains a highly covert crime and thus much of technology's impact might not be observable. For

example, the use of the Internet to effect money transfers has made it a lot easier to hide funds. Thus, in this sense, technology does facilitate corruption. However, the use of technology has had a dramatic impact in the prevention of corruption.

Before touching on prevention, however, it is important to recognize what ways technology operates in the perpetration and prevention of corruption. Concerning perpetration, many states are now making large purchases to maintain or improve their technology infrastructure, thus opening the door for kickbacks and other common forms of corruption. The other effect that technology has had is in promoting transparency. For example, the city of Seoul, South Korea, recently created online access to review permit applications and decisions on those applications, thereby enhancing transparency of the application process. This is a good example of how, through transparency, accountability and use of the Internet, one can begin to control the secretive nature of bribe paying and bribe taking.

The creation and enforcement of new laws concerning corruption has proven nothing short of incredible over the last three to four years. For example, the Foreign Corrupt Practices Act has a couple of interesting provisions that allows countries to seize or confiscate bribes as well as to prosecute the offenders. Furthermore, the Council of Europe in 1999 adopted a convention against corruption signed by 41 member states. A final example is the Inter-American Convention Against Corruption, signed by all of the Latin American countries, the US and Canada, which aggressively promotes international cooperation for the investigation and prosecution of corruption cases. It specifically states that bank secrecy cannot be used as a shield to prevent information sharing among member countries needed to prosecute a corruption case. The creation of such international tools are the frameworks from which the use of technology to oppose corrupt practice will grow.

The next speaker, **Dinkar Gupta**, provided an Indian perspective on the issues at hand. India has been slow, as an entire nation, to take to information technology, and even slower to catch onto the e-commerce movement. Yet, the information technology industry is becoming a more important part of the Indian economy, both in terms of domestic industry and those who travel abroad to work in the industry. Incidents of crime using technology are increasing, and Mr. Gupta focused his remarks on three problem areas.

The first area is criminal activity within the context of the Internet and computer systems. Software piracy is a major area of concern for India, as close to 90% of the software in India is pirated. India has also encountered cases of cybersquatting, and has seen some cases of men stalking women using the Internet and email programs. Turning to the criminals, Mr. Gupta noted that many of the same engineers being trained for the information technology industry have begun to turn to illegal activities on the Internet such as those mentioned above. While India has begun to respond to the problem, they have not yet had a trial in India concerning criminal activity through the Internet—though the first one is expected to occur in the summer of 2002.

The second area of concern is within the realm of computer networks, especially those controlled by the state. Since local and the central government rely on these computer systems for information and revenue exchange, they are ripe for criminal activity—mainly by insiders. One case Mr. Gupta outlined concerned the embezzlement of funds from the computer systems tracking government receipts from sales taxes. In order to conduct the scheme, the government inspector wrote his own software and loaded it onto the system. The most significant concern, in this regard, is that while official networks are moving into the digital environment, the legal and police resources to detect and respond to crime in the digital environment have not developed beyond their infancy, creating a yawning gap that criminals can exploit.

The final area of discussion was telecommunications, mainly concerning the use of cell phones. Criminals and organized crime groups often use cell phones as a way to communicate—even with those in jail for prior convictions. For example, a recent sweep of a major prison in New Delhi revealed 37 active cellular phones that criminals used to communicate with the outside. By increasing their institutional capacities in conducting telephone intercepts, the Indian police forces have become more adept at turning the tables on organized crime and terrorist organizations using cellular phones to communicate, but obviously these efforts must continue.

In Mr. Gupta's concluding remarks addressed the Indian response to the problem of cyber crimes. In terms of legislation, the Information and Technology Act of August 2000 added substantive criminal law and made India one of only 12 countries that have laws in place to address cybercrimes. In terms of institutional capacities, the Central Bureau of Investigation, a functional equivalent to the US Federal Bureau of Investigation, has taken the lead on investigating cyber crimes, and are also training state police forces in conducting investigations of this type. Finally, partnerships with private industry, mainly the National Association of Software and Service Companies, provide expert advice and guidance in investigating cybercrimes. In the end, Mr. Gupta noted that the Central Vigilance Commissioner in India, the chief investigating office for cases of corruption, is making great strides in employing technology to discover cases of embezzlement and other forms of corruption.

The last speaker, **Mikhail Vertuzaiev**, presented research he has conducted on reducing the exploitation of electronic transfers and smart cards by organized criminal groups in Ukraine for money laundering and theft. In 1999, Europay International began operations in Ukraine to coordinate the development of Maestro and MasterCard credit cards systems. The objectives of this association included the establishment and functioning of a collective security system, the coordination of inter-banking activities to prevent fraud perpetrated using plastic cards, and the promotion of interactions with law enforcement agencies. The association has also set up an international conference to achieve security in plastic card settlements as well as implementat a priority action plan to prevent fraud. An agreement has been signed on information exchange by a number of banks, and a database is being set up for merchants and cardholders which is basically a blacklist of private individuals and legal entities.

While the US has made good strides to prevent and control fraud, Ukrainian law enforcement has made no such efforts. While some articles exist in the Criminal Code to combat fraud and associated criminal activities exist in Ukraine, law enforcement agencies do not enforce them in the realm of credit cards. The majority of the anti-fraud efforts in Ukraine pertaining to in the context of credit cards are conducted by privately hired security services by commercial banks.

Dr. Vertuzaiev concluded his talk by noting that Ukraine needed to improve its international cooperation with law enforcement in order to combat many of the issues raised in the conference thus far.

Panel III Encryption and Privacy

The third panel focused on the critical interactions among transnational crime, corruption, and information technology. Encryption is often held out as the key advantage that criminals have over law enforcement. Law enforcement and the intelligence community are seeking to limit the strength of encryption keys, noting that encryption slows their investigation and could become unbreakable, thus allowing criminals and others to communication without fear of law enforcement listening in. Privacy advocates, on the other hand, support the need to ensure

private, legitimate communications and thus argue against limiting the strength of encryption technologies or providing law enforcement with keys that would allow them access to encrypted communications. The panelists, therefore, examined the merits of these arguments in the context of transnational crime and corruption.

The first speaker, **Dr. Dorothy Denning**, addressed how transnational organized criminals use encryption and associated technologies. Encryption, according Dr. Denning, is being used in many different contexts, various forms of communications, as well as in the storage of data. The evidence for the use and effects of encryption are currently anecdotal. New guidelines on reporting the results from wiretaps and the instances where encryption frustrates those wiretaps offer some hope for better data in the future. Turning to criminal activities, encryption is used in many different types of crimes, ranging from terrorism to narcotics trafficking and other forms of organized crime. One illustration involved a university professor who allegedly engaged in child pornography and the campus police could not do anything with the files on his computer due to strong encryption.

Thus, how does one approach cases that involve encryption? Breaking the method of cryptography or getting the key solves many such cases. Since a password often protects the encryption key itself, investigations often focus on acquiring the password and, in turn, the key to decoding the encryption. In many cases, the cryptography is broken not because the algorithms weren't of sufficient quality or the keys weren't long enough, but due to the overall weakness of products and the ability of "brute force" techniques to overcome the encryption—particularly true of most commercial software products until recently.

But encryption is not the only issue in this context. Steganography, for example, is related to and yet different from encryption in that encryption is extremely recognizable—one can recognize an encrypted file when one sees it. With steganography, one can hide files not only in images, but also in sound files, video, text, or even in unused space in a disk. Thus, you can use encryption with steganography for added protection and deception. Another issue is anonymity, where all kinds of services and tools exist to provide anonymous communications. Anonymous remailers, for instance, work with electronic mail to shield the source of electronic communications. Finally, the use of hacker tools, especially those designed to cover the tracks of email and to intercept passwords of user accounts, is a topic that one must consider when examining the use of encryption for illicit gains.

The next speaker, **Jay Wack**, sought to provide the private sector's point of view in the debate between privacy advocates and law enforcement in the encryption field. Focusing on the positive uses for encryption and the fact that privacy components require addressing, it is useful to liken the debate to a scale. On one side is law enforcement, which that would like to know what's going on all the time. On the other side is the individual, who would like to be able to be anonymous all the time. While this exaggerates the positions of the two sides to illustrate the contrast better, it is important to ask how does one craft an equitable and manageable solution that bridges the gap between the two sides?

In order to answer that question, one needs to start with some of the issues that form the engines driving the debate. For one there is issue of privacy itself, or "the right to be left alone." While simplistic, this statement merely reflects that privacy is a huge problem to contend with in this debate—especially in the US. The continued growth of the Internet and, especially, the connections between massive computerized information systems have led some industry captains to note that era of privacy is over. Hence, when we speak of e-commerce, one of the driving influences behind the collection of information, we must speak of security (i.e. the control and safety of information), confidentiality (i.e. the restriction of access to information), and privacy, or what an information collector does with the database after its creation.

Many dynamics of American Internet usage are changing affecting the debate. One is that the US no longer serves as the location for the preeminent groups of the Internet. Although the United States does have in excess of 100 million people using the Internet, this number does not represent the majority of Internet users any longer. Thus, we now must concern ourselves with the fact that we share the Internet with many nationalities simultaneously, and their policies on encryption will impact the debate we are outlining today. The US has laws pushing and/or forcing us into the electronic environment. For example, Medicaid is a paper-based system that takes 65 days to process, and thus we would like to move to an electronic mechanism that takes moments to process. An inherent element of the paper process is its privacy, with it the fact that the paper is folded up, put in an envelope, moved through the mail system. It is confidential in that the envelope prevents others from seeing the contents; and many laws protect the privacy of people's mail. The problem in moving to an electronic schema is that the medical community now has to provide a similar state of confidentiality as the envelope. Compounding this challenge is to ensure privacy in such a way that the information moves across the network and to make sure that a signature is applied in such a way that the person's actual identity is confirmed.

Thus, a conclusion drawn from the engines described above is that one has to have the means of protecting his or her information on the information highway. From the business side, then, the encryption industry is trying to develop strong software packages that protect digital information while at the same time maintaining the speed that is drawing more information to the Internet. In order to accomplish this, one has to have a secure platform and a secure authentication. It starts with who am I? For example, Bruce Snyder recently wrote an article on the issue of the electronic signature law passed in January 2000. Citing defects in the system, one of the solutions he suggested to strengthen security systems was that they should have a hardware device, and information should not be put on a drive in "soft" form that could lead to theft and abuse. Another solution to ensure privacy is that smart cards be used to harmonize information systems and hardware.

In the end, there are solutions available that accommodate the conflicting personal, organizational, and law enforcement interests with regard to encryption. Confidentiality should be under the control of the individual.

The concluding speaker on the panel, **Jim Kerins**, sought to outline the effects, positive and negative, of regulating the production and use of encryption tools and began by reminding the audience of some of the more relevant statistics from earlier in the day. First, that the US is no longer the dominant population on the Internet in terms of access or e-commerce. Next, regardless of whether commerce is business-to-business, business to consumer or consumer to government, there is a virtual environment that provides anonymity in commercial dealings that fraudsters have taken full advantage of. Thus, analysis of fraud is very useful in understanding the need to understand the crucial elements of the privacy debate.

Looking to the dark side of the Internet, it is clear that fraudsters like the Internet. First, it allows them to be more efficient and effective in what they do and creates difficulties for law enforcement in tracing transactions back to specific machines or addresses. Second, there has been a transposition of trust from the real world into the Internet world from consumers. In real terms, this amounts to companies losing 20 to 30 percent to fraud—numbers that can spell the end to companies given the tight margins in e-commerce. One recent statistic noted that fraud on the Internet represents 1.4 billion USD, or 11 percent of all e-commerce transactions. Thus, the most important engine to e-commerce fraud is that when you move from the real world to the virtual world, you can assume another identity that suits the fraudsters.

Turning to privacy, it is important to recognize that there are different types of information. First is accepted public information, such as telephone numbers or addresses, that people can now more readily access using the Internet. There is a very low expectation of privacy over these types of information. Public record information is another category of information. In the US, there are a lot of records that are maintained at the government level (e.g. federal, state or county) and available for public review, such as title records on property transactions. From the First Amendment standpoint, the information is public in order to allow for accountability and transparency of government activity. These particular types of information represent a challenge as it moves to a virtual environment. While knowing what one's neighbor paid for their house might not cause significant harm, a fraudster can use that sort of information to their advantage. Finally, there are types of information, which ought to remain confidential because of their potential use by those, engaging in fraud, such as medical records, financial information, and certain types of personal identification such as social security numbers.

There are important implications of privacy laws for businesses seeking to prevent fraud. The European Protection Act, provides a wealth of data for law enforcement while shielding it from businesses unless they become data providers. Individuals have the ability to opt out of data collections, which fraudsters are sure do as they wish to avoid inclusion in these databases. The US, recently addressed this issue in the Financial Modernization Act of 1999. The crux of the problem for business, however, is verification and validation. When a customer makes an e-commerce transaction, the business has mere seconds to try to validate the information and accept the order. Without the use of databases to validate the information that the customer is providing, fulfilling an order is reduced to an act of faith.

In conclusion, what are some potential recommendations? In this competing environment, there still needs to be access to information. This access actually helps protect confidentiality in some cases, but then there are all the other elements discussed earlier, such as the integrity of the data, the notification of the consumer and related parties, and the authorized access to information generally. However, from a fraud investigators standpoint, failure to provide access to data will diminish the ability to investigate, prevent or detect fraud and, in turn, will result in a fairly significant rise in economic crime. Finally, there also needs to be the capacity to share information for risk management and fraud detection purposes. If you have a series of individuals accessing multiple databases and committing crimes, including fraud, that information should be shared among banks or insurance companies. They should be able to warn each other that an individual is committing fraud against the company.

During the question and response session that followed the panel, the first issue that arose was that of liability for companies (i.e. the compilers) and individuals (i.e. the providers) with regard to exchanging credit card information in the virtual environment. Dr. Denning noted that individuals are not liable for credit card fraud with the guidelines established through their credit card providers, though if the information is used to further an identity theft scheme, it can create liability problems and, more importantly, it can compound the time and effort required for the victim to clear their credit rating. She added that while we currently treat social security numbers as a universal identifier in US financial markets, but the security lapses in using this system require that we adopt another system for authentication, such as biometrics or digital signatures. Mr. Wack noted that compilers of information from consumers are liable for maintaining the security of that information, and noted that, should criminals compromise biometric devices, it would lead to major identity theft problems as individuals would lose the ability to prove their real identity.

Panel IV Digital Networks

Concluding the examination of the ways that information technology, transnational crime and corruption interact, this panel sought to examine how illicit networked organizations, such as transnational criminal groups and terrorist cells, use information technology to organize and communicate. A central point concerning transnational networks is that, given the risk of law enforcement interdiction and the transaction costs from working internationally, they require swift, secure, reliable, and robust communications to maintain operations and that is what influenced the selection of the panelists and the issues addressed. Looking at this discussion from the other side entailed an examination of how governments and private institutions are using technology to identify illicit transactions and communications through surveillance and other means. The panelists, therefore, sought to identify the ways that digital communications assisted in transnational crime, the methods that law enforcement and others are employing to leverage these communications, and the broader implications of both of these activities.

Matthew Devost opened the panel by introducing the attributes of information terrorism, drawing on research that the Terrorism Research Center originally sponsored. In defining the issue, the study stated that information terrorism is not mischievous hacking for ego or financial gain, industrial espionage, electronic extortion or blackmail. Rather, it is a political crime attacking the legitimacy of a specific government, ideology, or policy. What this means is that it is rather difficult to address from a single perspective, such as law enforcement or military. Thus, you need to start with a coherent policy delineating roles and responsibilities to respond to the problem.

Continuing, what are the likely targets of an information terrorism campaign or attack. Here, it is useful to refer to a critical infrastructure threat matrix, which works as follows. If you are a terrorist organization that is looking to launch a terrorist attack using information technologies or not, it would fall into one of four categories:

A. Traditional conventional terrorism or use of a physical tool against a target (e.g. the Oklahoma City bombing)
B. Use of a physical tool against a digital target (e.g. the IRA attack on London's Square Mile in 1992)
C. Use of a digital attack tool against a physical target (e.g. spoofing air traffic control to crash a plane)
D. Use of an information or a digital tool against a digital target.

In (D), it becomes incredibly hard to determine if an attack is occurring, what the source of the attack is, or what the capabilities of the terrorist groups are that are out there.

Next, we must ask what some of the current threats are, and what we should expect to see as goals for the future. Some of the more traditional, or present goals include the unauthorized disclosure of data, the corruption of data, and a rather popular one—the denial of service. One could also look broader, including the disruption of communications technologies outside of the information network sector. Some future goals might include the disruption of the integrity of society, creating public panic and distrust by disrupting financial systems as examples that are seen in war games. Goals serve as insights into the style and tempo of current and future operations, and thus are a useful tool for analysis.

One analytical tool, formed from combining targets and goals, is the identification of potential actors. Criminal hackers are one such group as they are recruited for terrorist organizations. There are also the curious hackers who don't pose any real threat except that they are providing tools and capabilities that can be utilized by other groups. The sophistication of the hackers' tools and their user friendliness are increasing. Simultaneously, the basic level of

technical sophistication required to conduct information terrorism is decreasing. Other actors who can potentially engage in information terrorism include corporations and nation-states.

Another topic of discussion is the information technology tools that actors employ. Within terrorist groups, for example, digital information tools are proving themselves extremely useful such as mailing lists, private chat rooms, and encryption. These are important information tools to coordinate activities and to distribute propaganda. It is almost impossible to respond to widespread information terrorism attack.

Criminals and terrorists find these tools attractive for several reasons. First, information technology professionals and others in the US have continuously identified vulnerabilities in our network infrastructures and software that criminals can exploit. While in and of itself this is bad, but it also engenders fear that criminals and terrorists see as a vulnerability unto itself. Second, with these tools you have a significant capability to disrupt the lives of the citizenry. Third, it is very difficult to respond to these types of attacks.

In conclusion, what are some of the challenges that we must face given the existence of these tools and their use by illicit networks? First, developing a better understanding of the threat that faces us is important. For example, how can you differentiate between real attacks and false alarms? Second, building off of threat analysis, we need to develop warning and crisis management capabilities. In this regard, we need to move beyond host-based and network-based alarms and build into the realm of context-based intrusion detection because many of the emerging tools are not going to be easily detected. Further, we need to continue vulnerability analysis to understand weaknesses and improve the security of potential targets. Finally, we need to think of security as a design concept, leading to certification of technologies, business practices, policies and procedures as secure.

The next speaker, **Marc Zwillinger**, addressed network monitoring from two perspectives—that of the public and of the government. He opened by making some introductory points that largely drew on Mr. Devost's presentation. First is that little brother, all those non-governmental organizations such as employers, advertisers, and e-commerce sites that are monitoring network traffic, is larger than big brother, the government, in terms of who is conducting network monitoring. The government, in other words, plays a small role in monitoring network traffic. Second, government having the technological capacity to monitor does not mean that the government has the right to do it. The citizenry should not be alarmed that the government has a tool such as Carnivore. Third, sometimes monitoring can be a good thing. Examples of this include parents installing software on their computers so they can monitor their children's Internet usage.

There is far more concern with electronic monitoring than there is with phone monitoring. The reason for this is deeply rooted in concepts of monitoring. It is not inconceivable to you that someone can listen in on your phone call—for example; someone in your house can always pick up an extension and listen in on your conversation. But to some people it is inconceivable that they could be typing on their computer and someone else sees everything that they are doing. Furthermore, we love technology, and we want to consolidate as much information into as small and useful a platform (e.g. Palm Pilot) as possible. But the ability of others to interfere in the process of accessing that information or intercepting communications prevents us from adopting technology as quickly as we like.

We need to make a frank assessment of the some of the arguments on both sides of the privacy debate. While some will argue the government has too much access to personal information, the fact of the matter remains that the government is notoriously bad about stopping international cybercrime, and much of the reason for this lies in the tools available to the government. Computer facilitate only a small percentage of crime currently. Some of the cases

we have seen include computer intrusion, hacker, Internet gambling, cyberextortion, and some terrorist cases. Furthermore, it is quite clear that law enforcement agents are too quick to want to intercept data and to try to get a court order. What prevents those impulses from being acted out, however, are the requirements that those same agents prove to a judge that they could not collect the information they require through other means.

Network monitoring is the interception of data as it goes by. It is not the collection and post facto analysis of network traffic—a separate topic worthy of a separate discussion. The government uses two major methods for network monitoring-- pen registers and trap and trace. They are carryovers from the phone intercept realm. The majority of the information you receive from these methods is identification of who called whom, when, and for what duration. Due to the large amount of information that these techniques develop in the digital environment, they are not proving as useful as they have in the telephone realm.

In order to intercept content, law enforcement needs to follow the dictates of Title III or the Wire Tap Act, a law that says one cannot intercept electronic communications unless there was an issued order. Law enforcers can get this order if they can show probable cause that someone is committing or about to commit an offense. The law, however, permits private entities to intercept traffic almost at all times based on self-defense and consent. Examples of reasons why private entities engage in network monitoring include ensuring that confidential or privileged information is not being disclosed, or to maintain the ability to detect an intrusion into the system. Both are liability issues, as the last panel noted, for corporations. Furthermore, excessive network usage can reduce the productivity of a corporation, and thus many companies require a signed statement from employees that states that they understand that their Internet usage is subject to monitoring for inappropriate usage.

Thus, we have two types of monitoring, government and private, that involve different types of requirements to enact. Likely the most harmful types of monitoring are those that advertisers and e-commerce sites undertake to track the movements of consumers on the Internet to send you targeted mailings. Employer monitoring of employees, while often reflected on in a unpleasant light, is likely not so harmful since most people who work in an office environment do not have an automatic reasonable expectation to privacy in their personal space. For example, employees often share their physical workspace unless they have a locked file drawer that only they can access, and the employee's use of digital networks is no exception. Should you want to free yourself of an employer's network monitoring then, at the least, you have to provide your own computer and network access to create a reasonable expectation of privacy.

The next speaker, **Mike Godwin**, addressed the effects of network monitoring. Whenever a society is empowered to do things that they were never able to do before, it creates opportunities for new kinds of crime. Within the national context of combating cybercrime and other uses of digital networks for illicit ends, it is reasonable to adopt legislation that streamlines the law enforcement process to trace an intrusion or a criminal's e-mail through the various routes it might have traveled. Likewise, the international community needs to address these same issues given the wide distribution and empowering nature of personal computing, and the resulting empowerment of cybercriminals. It makes perfect sense for the international community to think in terms of adopting a streamlined procedure for searching and seizing communications and other kinds of data in the global context.

That said, we have to step back and think about the balance among the kinds of privacy valued in society, and the limitations on government valued in our society, and the ability of law enforcement to enforce legal codes. The problems are complicated by the fact that more and more individuals are empowered by these new technologies. This creates more of a threat to individual privacy and leads to a creeping set of government prerogatives that are not always

clearly constrained by legislative or other policy constraints. In the US, for example, the Fourth Amendment is the bedrock principle for searches and seizures of individuals, and if one has a computer at home and it is not hooked up to any network, then Fourth Amendment constraints still apply.[2] But, things change once the computer is connected to the rest of the world. Not only might you leave personal data on remote systems, it is also the case that the information that you are leaving is digital and hence profoundly searchable and analyzable. Because we store so much data in different places in digital networks, the presumption exists that it is really easy for law enforcement or private entities to gather that information without concern for privacy protections. Thus, it appears that when you look at how law enforcement communities discuss these issues, you see a split personality. Some say that "we have things under control," focusing on law enforcement's successes, while skeptics say that law enforcement requires more authority. The truth likely lies somewhere in between these two statements.

Criminals believe that they have a totally anonymous presence on the Internet. Past arrests show that law enforcement agencies can find, catch and bring them to justice. Criminals believe that they can intimidate companies with threats of computer hacking and the spread of malicious accusations. Global operations have shown that private industry can stand up for its property rights and does not have to submit to such blackmail. In conclusion, if we let the threats of international crime, domestic cybercrime and terrorism, lead us to empower law enforcement to invade our privacy without correspondingly creating increased privacy protections, we have let them win because we will have changed the values we cherish in response to their threats. Thus, we need to keep the notion of balance in mind as we move forward to address the proper amounts of and processes for network monitoring.

The final speaker on the panel, **Makon Delrahim**, examined the monitoring issue from the viewpoint of lawmakers.[3] Surprisingly, despite advancements in communications technology, Congress has not revisited the rules and authority for monitoring communications since 1986. Now, Congress is trying to catch up with technology. For example, Carnivore and its use by the FBI is beginning to raise policy questions concerning what legitimate rights the government has to the information that they collect and the appropriate balance with the privacy rights of citizens.

Quite simply, the problem is determining what is a reasonable expectation to privacy? The Constitution allows for a balance, but that balance can be unreasonable since it leaves it to the court to decide. In 1979, the Supreme Court stated that individuals did not have a right to privacy concerning the types of information that pen registers and trap-and-trace devices collect. This is what law enforcement relies on today for network monitoring. Obviously, privacy advocates and other groups argue that the technology has changed and thus a reassessment of law enforcement's tools and capabilities to infringe on the Fourth Amendment are worth a review.

While it may be up to the courts to decide this, Congress is looking forward to a healthy debate in the upcoming term on network monitoring tools for law enforcement versus privacy concerns. One important issue within this debate is in the realm of terrorism. On the one hand, law enforcement has stated that criminals and terrorists have outpaced them and that they need more tools to meet the challenge, whereas privacy advocates warn of severe erosion of civil

[2] The Fourth Amendment to the US Constitution states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

[3] It is important to note that Mr. Delrahim spoke in a private capacity and thus his remarks do not constitute the official views of the Judiciary Committee.

liberties from such a move. Thus it was important when CIA Director George Tenet recently testified that terrorist groups including Hezbollah, Hamas, the Abu Nidal Organization and Osama bin Laden's Al Qaeda are using computerized files, email and encryption to support their operations. This information is not likely a surprise, but it should give some persons concerned about their security pause. Espionage and information warfare also offer similar insights into this debate.

Some other issues have come to the attention of lawmakers. One of the more contested issues is the right of an employer to monitor the email and other digital activities of their employees, and the (potential) requirement for employers to notify employees of their monitoring policy. Another contested issue is third party records, where the government seeks access to individuals' holdings in network storage companies or Internet service providers.

These are some of the issues Congress expects to grapple with in the network monitoring debate. According to conventional wisdom, we have established eight levels of protection for network monitoring, moving from real time communications through various types of telephone and electronic forms. But it is an exciting time for new technology, and one anecdote that arose from hearings recently held was that when the automobile was invented, some people tried to ban it because it made bank robberies easier. We found a way to cope with that problem by providing law enforcement better tools than the criminals, and the hope is that both law enforcement and civil rights advocates will realize they are both being challenged by technology.

Some interesting issues arose during the question and answer session following the panel. The first discussion revolved around the regulation of the hacker movement. Mr. Godwin put forth that they are already regulated, in that writing malicious code like viruses, for example, is legal in that it improves our understanding of vulnerabilities and shortcomings, while releasing such codes to exploit these weaknesses is illegal. Mr. Delrahim added that we need to focus on negligence, often on the part of those individuals and companies operating information systems, rather than on gatherings of security people around the world, which continue to make valid contributions to securing information systems.

Another issue that arose was how to make the Internet more secure for the individual without threatening the individual or the larger. Mr. Delrahim noted that, from a legislative perspective, the US is encouraged that many other countries are taking sure strides to secure the intellectual property rights of their citizens. The US has focused on protection of intellectual property rights for individuals, identifying activities and protocols Internet service providers can undertake to reduce liability. However, First Amendment concerns in the US make it difficult to enact regulation on certain types of potentially fraudulent or otherwise criminal activity, such as the advertisement and sale of fake ID cards as novelty items. Mr. Zwillinger added that the US alone cannot make the Internet secure, due to it's international nature.

Panel V Finding Creative Solutions

Opening the second day of the conference, the fifth panel shifted the focus of the conference to how to answer the challenges identified during the previous day. The panel sought to explore just what solutions or mitigation strategies exist to hamper, curtail, or prevent information technology benefiting transnational crime and corruption. While examining the current tools available to address the situation, the panelists also sought to lend their insight on where they felt regulation was warranted or necessary to protect the public good.

The opening presentation from **Casey Dunleavy** and **Phil Williams** detailed the research they are conducting on network intrusions for the Computer Emergency Response Team (CERT). In their opening comments, Mr. Dunleavy stated that the ultimate goal of the study is

to create a methodology to proactively warn of threats on the Internet. For example, using a broad database, they are profiling the victims as well as the perpetrators in order to try to determine why somebody is targeted. Thus, the endgame is creating the ability to produce predictive intelligence and reduce damages.

The first thing the study considered is what kinds of malicious activity occur on the Internet currently. The Internet has disrupted military movements, and has the potential to do so again. More well known are the effects that criminal use of the Internet has had on business. For example, identity theft and stock manipulation are just some of the criminal activities facilitated through the Internet. As the Internet has become part of the social fabric, criminal activity disruptions on the Internet will impact all aspects of our day-to-day lives.

Through the analysis of roughly 1600 intrusion reports and other records, we are beginning to find patterns and starting to construct predictive analysis. For example, analysts had assumed that a six-week time period existed between the identification of a vulnerability in an information system and the implementation of a new intruder tool. However, what analysts actually found was that the time was closer to ten days. Thus, the means of communication between hackers, cybercriminals, and cyberterrorists is much better than the analysts had anticipated.

With that, Dr. Williams continued the presentation, opening with the thought that we are now at a stage of declining sophistication in hackers and a growth in sophistication in hacker tools. Yet we could soon face be another phase where the sophistication of hackers and their tools increase simultaneously. This, obviously, would be a real problem and five specific trends bear out this concern:

1. An overlap between organized crime and cybercrime. While they are never going to be congruent, organized crime will continue to engage in cybercrime and thus will engender an overlap between them. One can refer to this overlap as "transnational virtual crime."
2. A movement from nuisance to crime. While computer viruses cause annoyance, they can also cause major disruption and harm—the Lovebug virus, for example, caused an estimated $6 billion in damages and lost productivity. Further, viruses are becoming more specific in their targets and thus becoming tools for criminals.
3. The opportunities from cybertools give criminals and terrorists a weapon of last resort. Rather than having weapons of mass destruction, we see the creation of weapons of distributed destruction, as the bullet above noted.
4. Growing use of encryption. Encryption is a strategic defense initiative for the criminal world that fundamentally changes the playing field. It shields criminals from criminal tools like RICO and surveillance.[4]
5. Increasing exploitation of jurisdictional asymmetries. Through three different methods—arbitrage, voids, and confusion—criminals are exploiting the differences among criminal around the world to reduce the risks that law enforcement pose to them.

In conclusion, there are two models to deal with cybercrime internationally. One is the model of legal strategies developed from transnational organized crime law, calling for greater harmonization of laws, greater law enforcement cooperation, and the fostering of law enforcement networks. The other model is that applied to money laundering—naming and shaming offshore financial centers to influence their behavior. As one observes the growth of offshore information centers, governments will have to take the same kind of hard line towards them.

[4] RICO is the Racketeer Influenced and Corrupt Organizations statute, the main US weapon for attacking organized criminal entities.

The next speaker, **John Tritak**, addressed the importance of public-private partnerships in responding to threats from cybercrime. Partnerships are important because they enable the partners to better manage their risk in an information age. For the government, they help manage the risk posed to national defense, economic security, and the health and well-being of citizens. For the private sector, they help manage the risks to their businesses. In the end, it is clear that solutions based on public-private partnerships are preferable to those based on regulation regimes.

Regulation, therefore, is reserved for situations when the market fails and the government must step in. Thus, the next logical question is what risks we face for market failure, and here the Critical Information Assurance Office (CIAO) focuses on critical infrastructures. In the US, critical infrastructures are broken down into basic categories: information and communications, banking and financial services, transportation, electric power, oil and gas, and water. These infrastructures rely on information technologies, interconnected information systems, and networks to transact business as well as to perform core business operations and processes—including the operation of physical assets such as power plants and reservoirs.

The growing interconnected nature of these information systems into an ever-expanding digital nervous system is creating new vulnerabilities that, when combined with an emerging array of threats, poses unprecedented risks to national defense and national economies for countries all around the world. There is a great possibility that disruption of one enterprise in one sector will propagate a chain of failure, using the information highway as a conduit.

In 1998, Presidential Decision Directive 63 (PDD-63) was issued to address the potential vulnerabilities and risks posed to the critical infrastructures. It set out to develop a means by which to deal with those trends. PDD-63 called on each of the sectors to organize themselves and to ensure information sharing arrangements. Each sector is structured in similar fashions and therefore, to some extent, are similarly vulnerable to disruptions, especially in cyberspace. Information sharing helps them manage their risk by allowing information exchange concerning vulnerabilities. The arrangement helps develop a risk profile from the vulnerabilities that new technologies expose and, in turn, improves the ability of each sector to conduct strategic planning. Beyond intrasectoral information sharing arrangements, PDD-63 also called for cross-sectoral arrangements in order to identify those things that are unique and common to sectors and to manage risk accordingly. In this regard, there is a growing recognition that you can leverage a lot of very helpful and beneficial information sharing by crossing sectoral lines.

Moving on to discuss public-private partnering, the government has certain roles to play. One is to help support the information sharing process, especially in terms of providing information about higher-end threats that sector actors are not aware of, such as information warriors and terrorist groups. The other is to identify potential obstacles to information sharing or to investments that would improve information sharing, including such concerns as anti-trust violations or information sharing that exposes companies to civil litigation due to the public disclosure of vulnerabilities. In terms of public-private partnering in the cross-sectoral context, the most significant benefit the government can provide is as an enabler for industry to manage these problems in the cyber world.

In conclusion, Mr. Tritak felt that there is going to be a digital Exxon Valdez—a metaphor that serves to underscore the dangers of an interdependent, interconnected economy. This, above all, should prompt the public and private sectors to continue to cooperate. The other stakeholders that should be engaging in this process are the auditing, insurance, and investment communities. In sum, if they fail to deal with it, they actually may fail in their duties of due care and fiduciary duties, which expose them to personal liability. So, the idea is to start dealing directly with those people who actually make the decisions and the choices down the road.

Mike Orfini's remarks concluded the panel relaying the lessons from the Global Forum process on addressing corruption in the context of information technology.[5] The Global Forum was an initiative of Vice President Gore to create a major conference to discuss corruption thereby, creating a tool that could roll back corruption in governments without having a small minority of states cornering the high ground on the issue. Established with the help of the US State Department and others, the conference was a success as it hosted 500 people from 90 nations. In short, changes in the international environment meant that the time was right for an international meeting addressing corruption.

Since the late 1990s, the once-taboo topic of corruption began to enter the regular discussions among governments. The US, got an early start enacting the Foreign Corrupt Practices Act in 1977, making it a criminal offense for US firms to promise, offer or give bribes to officials of foreign governments to secure advantage in commercial transactions. Another watershed event was the adoption, in February of 1999, of the OECD's Convention Against Bribery of Foreign Public Officials. One other initiative is the 1994 Inter-American Convention Against Corruption. Hence, the Global Forum sought to harness this sea-change in the international community and further the development of international anti-corruption regimes.

The focus of the international community regarding corruption has shifted as a result of the Global Forum. The objective is now to help promote the visibility of other governments' efforts against corruption by promoting clear and objective international norms. While this objective has not yet been met, the Carter Center has followed up on this point by holding two conferences on corruption.

In the end, the success of the first Global Forum, held in February of 1999, led to the formation of a second Global Forum, set for May of 2001. Over 140 nations are expected to participate in the forum, whose ultimate objective is to work towards a United Nations instrument against corruption. Tying into the theme of this conference, information technology could be used to reduce the incentives, and the opportunities and increase the risk of exposure to corrupt practices.

Again, the question and answer session produced some interesting insights on the presentations from the panel. One discussion revolved around Dr. Williams' notion of encryption as a shield, and whether other forms of analysis—such as traffic or pattern analysis—might hold more useful data than the messages contained in the communications. Dr. Williams agreed, noting that analysts needed to think more strategically and use different analytic tools on the datasets. Another question arose about the level of technology around the world in the context of fighting corruption, and if we as Americans weren't recognizing the technological superiority we enjoy vis-à-vis other countries. Captain Orfini noted that, while the answer is not simple, they are aware of the problem and are working with aid organizations to try to rectify the problem.

In conclusion, the panel demonstrated that information technology offers solutions for many of the challenges posed by transnational crime and corruption. For example, Mr. Dunleavy and Dr. Williams suggested that analysts can use information technology as a tool to improve analysis and prevention of malicious use of software. In other cases, such as in the corruption realm, information technology offers the potential to enable or strengthen anticorruption regimes. Through creative solutions based on technology or through more traditional solutions enhanced through technology, the same types of technology can address the challenges arising from technology.

[5] For more information, go to www.gfcorruption.org.

Panel VI Identifying and Facing New Challenges

The final panel's focus addressed future challenges. Opening the panel, **Mary Riley** spoke on the corporate response to transnational crime and corruption using information technology. She began by reviewing some of the critical issues facing e-commercial operations, including intrusions and hacking, fraud, and regulatory and compliance issues (e.g. identity fraud). In order to combat these activities and others, it is critical that information technology security, fraud prevention, and security management officials within corporations come together and merge their skills to respond to the challenge.

But some other issues come into play when addressing challenges to e-commerce. For example, the speed of information technology greatly impacts the authentication of orders and identities. The ability of retailers to reconcile orders and authentication at such high speeds is incredibly difficult. Another area of concern is hacking and monitoring of secure communications, especially in the realm of online brokerages and banks. A final area of concern is extortion—the threat from hackers to damage or destroy the data banks of online retailers for ransom payments. For example, one hacker was able to insert code onto a retailer's website and, when his ransom request was not met, he took down the retailer's website—causing close to 400,000 dollars a day in lost sales.

The most significant threats, however, emanate from insiders. With increasing corporate mergers creating more disgruntled employees, the theft or destruction of secret information is becoming more prevalent. Such activity can often open corporations to lawsuits, and thus it is vital that corporations take steps to address this issue before it occurs, such as encrypting the information and securing their transmission. Finally, such a threat is leading to corporations and insurance companies cooperating more closely to share information and assess, right at the outset, how they are going to be protected down the road.

The next speaker, **David Von Vistauxx**, addressed what novel computer and communications technologies might appear in the future. It is simply astonishing to find how rampant the practice of repackaging old technology as "novel" or "new" is in the industry. There are ten points and trends that help to change the way we think about technology and its novelty:

1. Technology will change more rapidly in the future than it has in the past, and the rate of change in the future is faster.
2. People need to learn more about less—that is, people are expert on smaller issues because of the vast amount of information to sift through in today's and the future environment.
3. Communications and computers are going to continue to converge until they are, in his opinion, indistinguishable by 2007, a fact that raises serious issues for the future of technology security. Flaws in computerization, furthermore, will become flaws in communication.
4. While everything we do with computers or communications is becoming more complex at the operational level, it appears to be simpler at the user level.
5. Software will continue to become obsolete before it is debugged.
6. Today, less than 3% of delivered commercial software is peer reviewed (another professional programmer has reviewed the code for proper function and security) in the future this percentage is expected to drop even further.
7. Hardware innovation will continue to innovate at a geometric rate.
8. New technologies are becoming so complex that fewer people will understand them outside the design and programming teams.
9. Security continues to be an add-on rather than a design-in.

10. Security breaches are going to continue but the methods will increasingly become illegal around the globe.

In conclusion, two metaphors are useful when thinking about the future of computing and security—the moat and the Maginot line. The latter tried to keep the Germans out of France after World War I, it cost 8% of France's postwar GDP. The former was a large hole surrounding your castle and was not very expensive to construct. This difference is an enormous expense-but not in utility that the former worked for 6 hours—a massive waste of resources. Therefore, security must justify its expense.

The third speaker, **Lou Degni**, addressed future challenges law enforcement will face in addressing technology used by criminal organizations.[6] Unfortunately, while arming society with the tools of modern efficient communications, we have inadvertently armed the criminal element with those same tools. We are facing a very rapid deployment of technologies, and we realize there is an increased criminal use of digital technologies and the Internet. Furthermore, we have seen criminals undergo efficient paradigm shifts, for example moving from landline phones to cellular phones to new types of communications technologies. Unfortunately, you likely will not see government agencies and corporations shift as efficiently because criminals do not adhere to rules.

A series of serious challenges face law enforcement in the near future. First, what makes digital technologies attractive to criminals is the mobility they offer, which in and of itself poses difficulties for wiretapping as the wire rooms that monitor the taps now have to move with the communications devices. Due to digital transmission protocols, mobility and encryption, these devices pose challenges to law enforcement conducting lawful, authorized electronic surveillance, and thus require intercept techniques that are different from what law enforcement is used to. Second, law enforcement lacks the qualified personnel to address technologically-intensive operations. Third, law enforcement is not competitive price-wise in terms of salaries for technology engineers. Finally, law enforcement is having a difficult time providing updated training.

Turning to law enforcement responses, one is the Communications Assistance for Law Enforcement Act (CALEA), designed to ensure preservation of electronic surveillance capabilities. Implementation of the act is very difficult. For example, the act covers packet data, but provides no standards for its implementation. Another response is the formation of specialized units within the FBI and DEA to assist state and local agencies with electronic surveillance. Third is the National Infrastructure Protection Center that Mr. Vatis spoke of the day before. Finally, law enforcement is undertaking efforts to recruit and retain information technology professionals.

Turning to future developments, one of the likely trends is the increased deployment of packet networks, and thus law enforcement will need to develop packet intercept techniques, consisting of a sniffer to find the packets law enforcement needs and a shredder to identify destination, origination and direction-flow messaging. Furthermore, cooperation between law enforcement and private industry will have to increase to ensure success. Finally, law enforcement deployment of specialized equipment and training is a requirement for improving our ability to respond.

The final speaker, **Helena Plater-Zyberk**, presented the findings from a recent study from McConnell International that grouped states by their security risk in terms of e-readiness and national cybersecurity laws. The study addressed questions in 5 key categories—

[6] Mr. Degni was speaking as an individual and did not necessarily represent the opinion of the Department of Justice or the policy of the Drug Enforcement Administration.

connectivity, e-leadership, human capital, e-business climate, and information security—for 42 mid-level economies around the globe. One major conclusion is that a number of countries that significant shortcomings in their legal codes and law enforcement resources to deal with cybercrime.

The study of the state of cybersecurity laws around the world included information from 52 countries of differing economic levels. The data supported ten types of cybercrimes in four classifications:

- Data-related crimes: Interception, modification, and theft of data
- Network crimes: Denial of service and sabotage
- Crimes of access: Hacking, cracking, and virus dissemination
- Associated crimes: Aiding and abetting the above categories as well as computer-related fraud and forgery.

Over two-thirds of the country respondents did not have laws in place to prosecute cybercriminals whatsoever, and only one—the Philippines—had laws to deal with all ten.

The primary conclusion, therefore, is that far too many countries are relying on outdated statutes that predate the birth of cyberspace and have yet to be tested in court. Furthermore, laws are in place to protect government sectors without lending protection to the private sector. Finally, there is no model for what sorts of legislation need to be enacted.

Conclusion

The conference reached the following conclusions on five focal points from the introduction, and supported additional observations.

I. How does information technology facilitate transnational crime and corruption?

- Information technology is enabling transnational criminals and corrupt individuals to function more effectively
- Information technology is promoting the formation and operation of illicit networks by providing the swift and secure communications they require across vast distances
- Information technology is a revenue source for transnational criminals who use the internet and other technologies to commit fraud
- Government technology contracts are often the objects of corruption
- Information technology professionals in the software and computer engineering fields can also work, knowingly or unwittingly, for criminals in different regions of the world

II. How are trends in information technology affecting transnational crime and law enforcement?

- The growth of anonymity on the Internet benefits transnational crime groups and hampers the ability of law enforcement to trace communications back to a definite suspect
- The illicit networks of transnational criminals are adapting information technology faster and more efficiently than law enforcement.
- Hacker tools are becoming increasingly powerful tools of transnational criminals while the level of expertise required to operate them decreases
- Transnational criminals and terrorists are using the full range of technical means (e.g. encryption, steganography) to keep their communications protected from law enforcement

III. How does transnational crime affect current and new information technology, businesses and institutions?

- The convergence of information technology products (i.e. computers and telecommunications) in the future may lead to security holes which criminals can exploit
- Information technology in the hands of transnational criminals can undermine institutions and even governments

IV. Will new regulations in the information technology area cause more harm than good?

- Sharp regulations denying the ability of hackers to conduct licit activities could form a backlash in increasing security flaws for criminals to exploit
- Public-private partnerships are important in regulating information technology
- Regulation of technology must not impede innovation and technological innovation

V. Will regulation impact democratic processes and economic development?

- The private sector monitors networks more thoroughly and frequently than does the government. Privacy and civil liberty concerns must be addressed by both corporations and governments in achieving the necessary balance between regulation of technology and protection of the citizenry from transnational crime
- Limitations on encryption exports have tangible costs for U.S. technology firms. These costs must be weighted against the national security interests of the country
- Regulation of technology must balance the rights and civil liberties of individuals with the need to fight the harm caused by transnational criminals and corrupt individuals

Moderator and Speaker Biographies

John A. Beasley, Jr., *Assistant US Attorney, US Department of Justice Transnational/Major Crimes Section*

Mr. Beasley works at the Office of the US Attorney for the District of Columbia trying cases in both state and federal court. During his tenure he has held positions in the misdemeanor, felony, grand jury, narcotics, violent crime and transnational/major crime sections of that office, and for the last five years his work has centered on the investigation and prosecution of terrorism, espionage, export control and organized crime matters both in the US and abroad. He works closely in coordinating joint investigations between foreign and US law enforcement in Europe, Asia and Latin America. Before joining the Office of the US Attorney, he served in the US army judge advocate general's corps primarily as an instructor in constitutional law and international law subjects and as prosecutor from 1983 to 1987. Mr. Beasley graduated Boston University School of Law in 1983.

Walter D. Broadnax, *Dean, School of Public Affairs, American University*

Dr. Walter D. Broadnax is one of America's leading scholar-practitioners in the field of public policy and management. Prior to becoming Dean of the School of Public Affairs at American University, he was Professor of Public Policy and Management in the School of Public Affairs at the University of Maryland where he also directed The Bureau of Governmental Research. Dr. Broadnax has served as the Deputy Secretary and Chief Operating Officer of the US Department of Health and Human Services, President of the Center for Governmental Research, Inc., in Rochester, New York, and President of the New York State Civil Service Commission. He has held many positions including Director of the Innovations in State and Local Government Programs at the Kennedy School of Government at Harvard University; Director of Children, Youth and Adult Services for the State of Kansas; and Professor at The Federal Executive Institute in Charlottesville, Virginia. Dr. Broadnax received his Ph.D. from the Maxwell School at Syracuse University, his BA from Washburn University, and his MPA from the University of Kansas. He has also served on several corporate and non-profit boards of directors including the CNA Corporation, Keycorp Bank, Rochester General Hospital, Rochester United Way and the Ford Foundation/Harvard University Innovations in State and Local Government Program.

Vladimir Brovkin, *Director, United Research Centers Project, Transnational Crime and Corruption Center, and Associate Research Professor, School of International Service, American University*

Dr. Vladimir Brovkin manages the daily operations of the Transnational Crime and Corruption Center's (TraCCC) overseas research centers in Russia and Ukraine. He was the Principal Investigator for TraCCC's 1999 Money Laundering and Front Companies project. In addition to his work for TraCCC, Dr. Brovkin was a NATO Research Fellow from 1997-1999, and is currently the Executive Editor of three journals: *Organized Crime Watch-NIS, Demokratizatsiya*: *The Journal of Post-Soviet Democratization*, and *Organizovannaya Prestupnost i korruptsiya* (Organized Crime and Corruption) in Russia. He has served as a consultant for various US Government agencies on Russian and Post-Soviet affairs, and has delivered numerous lectures and participated in many panel discussions on Russian and Eurasian politics, organized crime, and corruption. Dr. Brovkin has published extensively on Russian affairs in major scholarly journals. He has also published several books on Russian political parties, including the acclaimed *Russia after Lenin: Politics, Culture, and Society* (Routledge 1998). Dr. Brovkin came

to TraCCC from Harvard University where he had been teaching Russian history and politics as an Associate Professor for seven years.

Mark Childers, *Special Agent, US Secret Service, Financial Crimes Division*
Mr. Childers has served in the US Secret Service for 5 years, and currently works in the Financial Crimes Division, where he oversees and manages ongoing criminal investigations in the field. Prior to joining the Secret Service, he served as a Deputy US Marshal for 8 years.

Louis Degni, *Special Agent, US Drug Enforcement Administration*
Special Agent Louis Degni has been with the Drug Enforcement Administration for 14 years. He has worked in New York, Miami and extensively overseas. Special Agent Degni has spent the last 10 years working in electronic surveillance. Currently, he is unit chief for the Wireless Communications and Emerging Technologies Unit of the Communications Assistance for Law Enforcement Act (CALEA) Implementation Section.

Makan Delrahim, *Counsel, Committee on the Judiciary, United States Senate*
Makan Delrahim joined the majority staff of the Senate Judiciary Committee in 1998 as Counsel. He currently oversees the full Committee's E-commerce, Antitrust and Emerging Technology Policy Unit. Prior to joining the Judiciary Committee, Mr. Delrahim practiced law at the Washington, DC offices of Patton Boggs, LLP, focusing his practice on intellectual property and international transaction and public policy matters. Before that, Mr. Delrahim was employed at the National Institutes of Health's Office of Technology Transfer, and in 1994 he served as Deputy Director for Intellectual Property Rights at the Office of the US Trade Representative, Executive Office of the President. Mr. Delrahim has co-authored two *amicus* briefs submitted to the US Supreme Court: one on the constitutionality of physician-assisted suicide, and the other on the international application of US Copyright laws. Mr. Delrahim holds a BS from the University of California, Los Angeles, and a JD from the George Washington University School of Law. He has successfully completed the requirements for a Master of Science degree from Johns Hopkins University in Biotechnology. He is a member of the California and the Washington, DC bars and is a registered patent attorney qualified to practice before the US Patent and Trademark Office.

Dorothy E. Denning, *Professor of Computer Science, Georgetown University, and Director of the Georgetown Institute for Information Assurance*
Dr. Denning specializes in information warfare and information assurance. Before going to Georgetown in 1991, Dr. Denning was a member of the research staff at Digital Equipment Corporation, a senior staff scientist at SRI International, and an associate professor at Purdue University. She is presently a member of the President's Export Council Subcommittee on Encryption Policy, a CINCSPACE CND/CNA advisory committee, the CSIS Cyber Threats of the Future task force, and Georgetown's Technology Oversight Committee. Dr. Denning is author of *Information Warfare and Security* (Addison Wesley, 1999), and *Cryptography and Data Security* (Addison Wesley, 1982), as well as over 100 articles. She is co-editor of *Internet Besieged: Countering Cyberspace Scofflaws* (Addison Wesley, 1998). She has testified before the US Senate and House of Representatives and is a frequent lecturer at conferences and symposia. She is an ACM Fellow and has received the National Computer Systems Security Award and the Distinguished Lecture in Computer Security Award. In April 2000, she was named the TechnoSecurity Professional of the Year at TechnoSecurity 2000. Denning received

BA and MA degrees in mathematics from the University of Michigan and her Ph.D. in computer science from Purdue University.

Matthew G. Devost, *Senior Information Security Analyst, Security Design International Inc.*
Matthew G. Devost has been researching the impact of information technology on national security since 1993. A founding Director of the Terrorism Research Center, Inc., an institute dedicated to research and analysis of issues in counter-terrorism and information warfare, he has provided support on information operations and information terrorism to the Department of Defense community, Presidential commissions, and other government, law enforcement and intelligence agencies. He also provides information security consulting and intelligence analysis for private corporations, including Fortune 500 companies and critical infrastructure owners. Mr. Devost has appeared on CNN, MSNBC, NPR and Australian television as an expert on terrorism and information warfare. He has lectured and/or published for the National Defense University, US intelligence and law enforcement communities, the Swedish government, Georgetown University, as well as in the popular press. Mr. Devost holds a BA degree from St. Michael's College and an MA from the University of Vermont.

Casey Dunleavy, *Member of Technical Staff, Software Engineering Institute (SEI), Carnegie Mellon University*
Mr. Dunleavy specializes in strategic analysis of threats to computer networks. A significant part of his work involves analysis of transnational organized crime as well as other potential threat groups. Prior to working at SEI, he was Chief, Computer Network Warfare Analysis, for US Space Command and the North American Aerospace Defense Command in Colorado Springs. He has also worked for the Office of Naval Intelligence, the National Security Agency, and other intelligence agencies. During a long intelligence career, Mr. Dunleavy has been recognized for work in the areas of strategic military analysis, ballistic missile defense, computer network security, indications and warnings, and crisis response. In addition to his analytic work he is a frequent guest lecturer and instructor on strategic military issues.

Mike Godwin, Policy Fellow, *Center for Democracy and Technology*
Noted Internet lawyer, activist and author Mike Godwin has extensive involvement with the legal and social issues affecting cyberspace. He served for nine years as staff counsel at the Electronic Frontier Foundation. Currently, in addition to his role as CDT policy fellow, he is Chief Correspondent for IP Worldwide and Columnist for American Lawyer Magazine, both publications of American Lawyer Media. Godwin has authored numerous articles and the highly-acclaimed book, Cyber Rights: Defending Free Speech in the Digital Age (Random House/Time Books, 1998). His writings and activism have covered issues as diverse as electronic search and seizure, free speech in electronic communications, and the affects of international law on computer communications. His discussions of the Internet's social and legal ramifications have appeared in the Whole Earth Review, The Quill, Index on Censorship, Internet World, and WIRED.

Louis Goodman, *Professor and Dean, School of International Service, American University*
Louis Goodman researches institutions of power that affect prospects for development in the third world. He is the author of numerous scholarly books and articles. His *Small Nations, Giant Firms: Capital Allocation Decisions in Transnational Corporations* (Holmes and Mier, 1987) discusses the determinants of capital allocation decisions in transnational corporation and the impact of transnational corporations on national development. *The Military and Democracy in*

Latin America (D.C. Heath-Lexington, 1990) and *Lessons from the Venezuelan Experience* (Johns Hopkins, 1995) are volumes he has recently co-edited which focus on the role of the military in political and economic development. His publications also include works on international affairs education including *International Affairs Education on the Eve of the 21st Century* (APSIA, 1994). Louis Goodman has been Professor and Dean of the School of International Service since 1986 and in 1992 served as the President of the Association of Professional Schools of International Affairs. Prior to assuming this position, he directed the Latin America Program at the Woodrow Wilson International Center for Scholars, the Latin America and Caribbean Program at the Social Science Research Council, and served on the faculty of Yale University. He received his MA and Ph.D. from Northwestern University and his BA from Dartmouth College.

Michael Hershman, *Chairman, Decision Strategies/Fairfax International, LLC (DSFX)*
Michael Hershman is an internationally recognized expert in areas relating to economic crime and computer security. As President of The Fairfax Group for more than 15 years, Mr. Hershman has managed highly sensitive investigations and security issues for governments and private sector clients. Immediately prior to founding The Fairfax Group in 1983, Mr. Hershman served as Deputy Auditor General for the Foreign Assistance Program of the US Agency for International Development. In the 1970s, he was selected by the US Congress as Senior Staff Investigator with the Senate Watergate Committee and then as Chief Investigator for a joint Presidential and Congressional commission reviewing state and federal laws on wiretapping and electronic surveillance. Following two years as Federal Election Committee Chief Investigator, he was appointed Deputy Staff Director for the Subcommittee on International Organizations of the US House of Representatives. This committee was responsible for legislation and oversight relating to international banks and other US supported international organizations, such as the United Nations. Mr. Hershman is a co-founder of Transparency International, an independent, not-for-profit coalition against corruption in international business transactions; a member of the US Chamber of Commerce Economic and Security Working Group; a member of the Partnership for Critical Infrastructure Protection; a member of the Fairfax County Board of Supervisors Audit Oversight Committee; and is on the Board of Editors of *The Journal of Proprietary Rights*.

James P. Kerins, III, *President, National Fraud Center (NFC)*
Mr. Kerins is responsible for the strategic decisions and partnerships of NFC. Prior to that he served as the Chief Operations Officer and Executive Director/Director of Investigations, with responsibility for management of all investigation and research activities throughout the company. Mr. Kerins has spent over 14 years with the National Fraud Center and has formal law enforcement experience and extensive professional training credits. Mr. Kerins holds a degree in political science and criminalistics and is currently a candidate for a master's degree in Economic Crime Management from Utica College of Syracuse University. He is a member of several organizations including the Council of International Investigators, where he has served as the President and Chairman of the Board. He also has received extensive certification in bank fraud, insurance fraud, and corporate fraud and is a Certified Fraud Examiner.

Nanette S. Levinson, *Associate Dean and Associate Professor of International Relations at the School of International Service, American University*
Nanette S. Levinson has written and lectured extensively on international communication and organizational change as well as on international science and technology issues. Dean Levinson's work cuts across several disciplines including sociology, political science, and

management. Her current research includes a comparative study of institutional change and Internet technology in the context of globalization, and her research and teaching has led to consulting assignments in both private and public sector organizations including the Xerox Corporation, the Department of the Navy, and the State of New Jersey. The Association of Professional Schools of International Affairs recently selected Dean Levinson to direct an international symposium on the use of telecommunications technologies in international affairs education. Having served as Chair of the Board of the National Conference on the Advancement of Research, she is also on the Board of the Women's Foreign Policy Group. Dean Levinson recently completed work on a study of women as leaders in international affairs sponsored by the Women's Foreign Policy Group and funded by the Ford Foundation. She received her BA, MA and Ph.D. from Harvard University in Cambridge, Massachusetts.

Captain Mike Orfini (USN), *Military Advisor for National Security Affairs to the Vice President*
A Naval Aviator, Mr. Orfini has been serving as the Military Advisor for National Security Affairs to the Vice President since 1996. He is responsible for advising the Vice President and his National Security Advisor on Western Hemisphere issues and on global programs on anti-corruption, environment, intelligence, natural disasters, counternarcotics, counterterrorism, and organized crime. Prior to this assignment, he served in many US Navy operational units including Commanding Officer of an aviation squadron in Florida. Born in New Jersey in 1955, Mr. Orfini has an undergraduate degree from Villanova University, masters degrees from the University of Southern California and Harvard University, and has completed an Executive Fellowship at the Center for International Affairs at Harvard University.

John T. Picarelli, *Analyst, Transnational Crime and Corruption Center (TraCCC), American University*
Mr. Picarelli is currently developing a law enforcement training curriculum addressing the trafficking of women and children and enters his third year of research on the relationships between transnational criminal organizations and information technology. Prior to joining TraCCC, Mr. Picarelli served as an analyst at Pacific-Sierra Research Corporation (now Veridian-PSR), conducting and briefing research to the defense and intelligence communities on organized crime, terrorism, and the proliferation of weapons of mass destruction. His most recent publications include "Information Technologies and Transnational Organized Crime," co-authored with Dr. Phil Williams, in Dan Papp (ed.), *Information Age Anthology, Vol. II* and an upcoming article in *Transnational Organized Crime* arguing that US law enforcement's atavistic employment of information systems hampers its abilities to mitigate transnational organized criminal enterprises. Mr. Picarelli is a Ph.D. candidate at the School of International Service at American University, earned his MA in International Affairs from the Graduate School of Public and International Affairs at the University of Pittsburgh, and his BA in International Relations from the University of Delaware.

Helena Plater-Zyberk, *Director of Research, McConnell International*
Ms. Plater-Zyberk assists private and public sector clients by creating strategies to reduce national-level information security risks and by evaluating countries' and regions' e-market potential and the viability of business opportunities within them in comparison with other selected economies or regions. Recently, she researched and analyzed the capacity of over 40 nations to participate in the global networked society, and presently she is engaged in a project to evaluate the laws of over 50 countries to determine governments' ability to prosecute cyber

criminals. Before joining McConnell International, Ms. Plater-Zyberk analyzed corporate governance trends in European markets at the Investor Responsibility Research Center and served as a Faculty Advisor to the National Youth Leadership Forum on Defense, Intelligence, and Diplomacy. As a Rotary International Ambassadorial Scholar, Ms. Plater-Zyberk earned a certificate in the Management of International Joint Ventures at the European University (Viadrina, Germany) and earned her BA in International Relations and Economics, cum laude, from the American University, School of International Service.

Mary K. Riley, *Director, Digital Risk Management, Price-WaterhouseCoopers Investigations LLC.*

Ms. Riley, now a Director of Price-WaterhouseCoopers Investigations LLC in Washington, DC, recently completed a 13-year career as a federal agent at the US Secret Service, resolving criminal investigations involving electronic crimes, network intrusions and financial crimes. She established and managed one of the largest computer forensic programs in law enforcement and has a reputation as a leading expert and innovator in the development of tools and techniques used in the investigation of high-tech criminal activity. Ms. Riley's law enforcement experience was built on a background in personal computer system integration at IBM and programming/systems analysis experience at the Army Corps of Engineers. She was able to join President Clinton and Vice President Gore in the introduction of the International Crime Control Strategy to a live international press conference audience including cabinet members, House and Senate congressional leaders and the directors of all federal and military law enforcement agencies. Ms. Riley drafted the Wireless Telephone Protection Act of 1998. She served as liaison to the telecommunications industry lobbyist organizations, the Business Software Alliance, and the House and Senate legislative counsel representatives, to ensure the bill's language had the desired effect for all parties. She also coordinated the investigation and computer forensic examinations of the 1998 network intrusion into the Nynex telecommunications network in Boston, Massachusetts.

Louise Shelley, *Director of the Transnational Crime and Corruption Center (TraCCC); and Professor, Department of Justice, Law, and Society, and the School of International Service, American University*

Dr. Shelley is a leading US expert on crime, law, and law enforcement in the former Soviet Union, as well as an expert on transnational organized crime and corruption. Since 1995, Dr. Shelley has conducted the TraCCC program in coordination with specialists in Russia and more recently in Ukraine on the problem of organized crime and corruption. As an advisor to the US government on the problems of post-Soviet organized crime, Dr. Shelley has testified before the House International Relations Committee on several occasions, most recently before the House Banking Committee regarding the Bank of New York. She is the author of *Policing Soviet Society* (Routledge 1997), as well as numerous articles and book chapters. Dr. Shelley is presently co-editor of *Demokratizatsiya*, the journal of post-Soviet democratization, and *Trends in Organized Crime*. Dr. Shelley received her undergraduate degree (cum laude) from Cornell University in Penology and Russian Literature. She holds an MA in Criminology from the University of Pennsylvania. She studied at the Law Faculty of Moscow State University on IREX and Fulbright Fellowships, and holds a Ph.D. in Sociology from the University of Pennsylvania. She is the recipient of Guggenheim, NEH, Kennan Institute and Fulbright fellowships and received a MacArthur Grant to establish the Russian Organized Crime Study Centers.

Alexis Slebodnick, *Senior Intelligence Analyst, CyberSmuggling Center, U.S. Customs Service*
Alexis Slebodnick is currently assigned to the CyberSmuggling Center's Child Exploitation Unit. As the Senior Analyst, she develops investigations into child pornography and refers cases to the appropriate field office. Ms. Slebodnick has been an intelligence analyst for eighteen years and was previously with the FBI and the Financial Crimes Enforcement Network (FinCEN). Her varied experience has included terrorism, drug, money laundering and Internet investigations. She received her BS in Business from Radford University and her MA in International Transactions from George Mason University.

Timothy P. Trainer, *President, International AntiCounterfeiting Coalition (IACC)*
Mr. Trainer assumed the position of President of the Washington, DC based IACC in September 1999. He oversees the IACC's day-to-day administrative operations, including its domestic and international programs. Prior to joining IACC, Mr. Trainer was an attorney in the US Patent and Trademark Office's (PTO) Office of Legislative and International Affairs for over three and a half years. He worked primarily on enforcement and trademark issues. As a PTO attorney, he regularly represented the United States at the World Intellectual Property Organization (WIPO), provided intellectual property technical support to the Office of the US Trade Representative and other US government agencies regarding intellectual property issues. Mr. Trainer regularly developed and coordinated intellectual property enforcement programs for WIPO, the US Department of Commerce and other US agencies. While at the PTO, Mr. Trainer's primary geographic areas of responsibility for enforcement matters were Asia and Europe. He has also worked in the Intellectual Property Rights Branch of the US Customs Service and practiced law in the Washington, DC office of Arter & Hadden. Mr. Trainer's articles have appeared in numerous professional journals, including "Copyright World," "Trademark World," "Trademark Reporter," "AIPLA Quarterly Journal" and "Managing Intellectual Property." His book, *Border Enforcement of Intellectual Property*, was published by in January 2000. Mr. Trainer received his law degree from the Cleveland Marshall College of Law in 1986. He also has an MA in Asian Studies from the University of Pittsburgh. Prior to his graduate studies at the University of Pittsburgh, he studied at Keio University's International Center in Tokyo in 1978-79.

John S. Tritak, *Director, Critical Infrastructure Assurance Office (CIAO)*
As Director of CIAO, John Tritak is responsible for supporting the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism in the development of an integrated National Infrastructure Assurance Plan. As Director, he will also coordinate a national education and awareness program, as well as legislative and public affairs initiatives. Before joining CIAO, Mr. Tritak was an attorney with the law firm of Verner, Liipfert, Bernhard, McPherson and Hand, Chartered, providing advice and counsel to domestic and international clients in the defense, telecommunications, and transportation industries. Mr. Tritak served as Deputy Director for Defense Relations and Security Assistance in the State Department's Bureau of Politico-Military Affairs, coordinating U.S. efforts in security assistance and the defense trade in Europe, Africa, and the Middle East. Mr. Tritak also served as a State Department adviser to the US delegation negotiating the Strategic Arms Reduction Treaty in Geneva, Switzerland, and was a deputy political adviser to US Central Command in Riyadh, Saudi Arabia, during Operation Desert Shield. He previously served as a consultant on national security and military matters at Pacific Sierra Research Corporation (now Veridian-PSR). Mr. Tritak received a BS in political science from the State University of New York, Brockport, an MA in War Studies from the University of London, Kings College, and his JD from the Georgetown University Law Center.

Michael Vatis, *Director, National Infrastructure Protection Center, Federal Bureau of Investigation*
Prior to becoming Director of the National Infrastructure Protection Center in February 1998, Mr. Vatis served as Associate Deputy Attorney General and Deputy Director of the Executive Office for National Security in the Department of Justice. In this capacity, he advised the Attorney General and the Deputy Attorney General on national security matters and coordinated the Department of Justice's national security activities. Mr. Vatis has also served as a Special Counsel in the Department of Defense and as a law clerk to the late Justice Thurgood Marshall of the U.S. Supreme Court and then-Judge (now Justice) Ruth Bader Ginsburg of the U.S. Court of Appeals for the D.C. Circuit. Mr. Vatis has also worked as a lawyer in private practice in Washington D.C. Mr. Vatis is a magna cum laude graduate of Princeton University and Harvard Law School.

Mikhail Vertuzaiev, *Professor and Senior Research Fellow, National Academy of Interior Affairs of Ukraine*
As a professor since 1995 in the Department of Forensics and a Senior Research Fellow at the National Academy of Interior Affairs of Ukraine, Mikhail Vertuzaiev's research interests center around issues of combating crime and information resource management in law enforcement. He was made a Member of the International Slavic Academy of Sciences in 1998. His other affiliations include the Scientific and Technical Council of the Prominvestbank of Ukraine. Vertuzaiev has presented the results of his study on financial safety in banking systems at several international conferences and has published extensively. His written works include *Computer Crime in Ukraine: Myths and Reality* (1997), *Use of Computers in Law Enforcement* (1996), and *Principles of Computerization for Law Enforcement Agencies* (1993). He earned his Doctor of Engineering Science degree from the Academy of the MIA of the Russian Federation in 1993. He holds a second specialized doctorate in management of technical systems.

David von Vistauxx, *Trelex Associates, Ltd.*
Mr. von Vistauxx has over 30 years experience in computer and communications security. He has extensive experience in satellite communications and networking, and has been an invited speaker at several international security symposia. He wrote industry standard device drivers for Optical Media for the UNIX operating system, and has co-authored texts on the Linux Operating System. Prior to Trelex, Mr. von Vistauxx was responsible for communications security for American Communication & Computation, Inc. in Washington, DC, and was responsible for maintaining an international rapid response capability for International Digital Maintenance, Ltd., also in Washington.

Jay Wack, *Chief Technology Officer, TECSEC*
Mr. Wack brings 25 years of extensive experience in the electronics and information security industries, primarily with the Avnet Corporation, to TECSEC's management team which he joined in 1992. He held positions in sales, sales management (including sales and service responsibility for 35 locations and 400 marketing and field engineers), technical sales support, marketing, engineering, operations, and product development. Mr. Wack's experience and contacts span both the commercial and federal markets.

Phil Williams, *Director, Matthew B. Ridgway Center for International Security Studies*
Dr. Phil Williams is Director of the University of Pittsburgh's Ridgway Center for International Security Studies and Professor in the Graduate School of Public and International Affairs at the

University. He has published extensively in the field of international security including *Crisis Management* (1976), *The Senate and US Troops in Europe* (1986), and (with Mike Bowker) *Superpower Détente: A Reappraisal* (1987). During the last six years his research has focused on transnational organized crime and drug trafficking, and he has written articles on these subjects in *Survival, Washington Quarterly, The Bulletin on Narcotics, Temps Stratégique, Scientific American,* and *Criminal Organization*. In addition, he is editor of a journal entitled *Transnational Organized Crime*. He has been a consultant to the United Nations on organized crime, drug trafficking, and money laundering. He has edited a volume on *Russian Organized Crime* and, most recently, a book on *Illegal Immigration and Commercial Sex: The New Slave Trade*. He is currently preparing a book for Polity Press on *Transnational Organized Crime.*

Vic Winkler, *Principal Architect for Security, Sun Microsystems Federal*
Vic Winkler has over 20 years of experience in Information Security (INFOSEC), information systems design, operations, implementation, and testing. He is a published author and researcher in INFOSEC, and an expert in intrusion/anomaly detection in complex systems. Currently, on the staff of the Chief Technology Officer at Sun Microsystems Federal, he is the Principal Architect for Security. In his present capacity, he is responsible for enabling customer security architecture decisions, authoring security whitepapers, and has written the security policy for the Government of Malaysia. He is a member of the Sun Board for defining the internal "Network Security Ambassador" program. He is the Sun technical representative to the Technology Working Group for the Center for Strategic and International Studies (CSIS) commission for reforming US information technology export control policy. Previously he represented Sun on the Steering Committee for the Information Systems Security Board (ISSB, spin-off of NSTAC Presidential NII Task Force). At Litton PRC Inc., he was a Principal Engineer on the PRC National Systems staff. He spent nine years as a technical member of the PRC R&D staff where he was the Principal Investigator for a number of R&D efforts in INFOSEC.

Marc J. Zwillinger, *Partner, Kirkland & Ellis*
Mr. Zwillinger is the leader of the Cyberlaw and Information Security practice group at Kirkland & Ellis and a member of the firm's Technology Committee. Prior to joining Kirkland & Ellis, he worked in the Computer Crime and Intellectual Property Section of the Criminal Division of the Department of Justice (DOJ). At DOJ, he coordinated the investigations of several high-profile computer crime cases including the 1997 penetration of US military computer systems by an Israeli hacker; the Denial of Service Attacks that hit e-commerce sites in February 2000; and the Love Bug virus. He also investigated and prosecuted cases involving violations of the Economic Espionage Act of 1996 (EEA) and was responsible for coordinating DOJ's approval for charges filed nationwide under the EEA. He personally represented the government in United States v. P.Y. Yang, et al., the first EEA case successfully tried in the US. He has trained hundreds of federal prosecutors and agents at the FBI Academy and at the Department of Justice's National Advocacy Center. In private practice, he now provides advice and counsel on protecting the confidentiality, availability and integrity of proprietary information, and conducts internal investigations and litigation for companies that have suffered a breach of computer security or loss of trade secret technology. He also helps companies help assess and limit their risk resulting from e-commerce related activities. He has lectured to a wide variety of audiences on topics related to computer crime and economic espionage and serves as an Adjunct Professor of Cyberlaw at the Columbus School of Law at the Catholic University of America. He was recently named co-chair of the Computer and High-Tech Crime Subcommittee of the White Collar Crime Committee of the American Bar Association. He received a JD, magna cum

laude, from Harvard Law School in 1994 and his BA in Political Science from Tufts University in 1991.

About the Transnational Crime and Corruption Center

Originally founded in 1995 with seed money from the MacArthur Foundation and the United States Government and funded by U.S. Government and private foundations, our basic goal is to better understand the causes and scope of transnational crime and corruption and to propose well-grounded policy. Much of our work to date has focused on the analysis of transnational organized crime and corruption in the countries of the former Soviet Union. To accomplish this, we work with the public, media, law enforcement, policymaking, legislative, judicial, academic and business communities. To undertake this kind of collaborative work, we have partnered with the best scholars and practitioners in Russia and Ukraine through multidisciplinary research centers. Future plans include a research project on money laundering in Georgia, Chinese organized crime in the United States and training curriculum on smuggling/trafficking for American law enforcement, while also continuing to work with colleagues in European, Latin America, Asia, and Africa.

We also advise numerous American and multilateral governmental and non-governmental organizations engaged in studying and combating transnational crime and corruption. These include the U.S. Departments of Justice, State and Treasury; the U.S. Congress; the Asia Foundation; the Korean Government; Transparency International; the Organization for Economic Cooperation and Development (OECD); the United Nations; the Organization of American States; the International Organization for Migration; the U.S. armed services; and the World Bank; as well as numerous US and international scholars, practitioners and advocacy groups. TraCCC hosts visiting scholars and international visitors throughout the year.

TraCCC and its local affiliates have co-sponsored seminars and roundtable discussions, instituted collaborative research, developed partnerships, and established an extensive database of colleagues in many disciplines in order to maintain dialogue among members of the international community concerned with the political, economic and societal cost of transnational crime and corruption.