EXPLORING MONEY LAUNDERING VULNERABILITIES THROUGH EMERGING CYBERSPACE TECHNOLOGIES

A CARIBBEAN-BASED EXERCISE

David A. Mussington / Peter A. Wilson / Roger C. Molander

Critical Technologies Institute

RAND
The research described in this report was conducted by RAND's Critical Technologies Institute.

ISBN: 0-8330-2665-8

RAND is a nonprofit institution that helps improve policy and decisionmaking through research and analysis. RAND's publications do not necessarily reflect the opinions or policies of its research sponsors.

© Copyright 1998 RAND

All rights reserved. No part of this book may be reproduced in any form by any electronic or mechanical means (including photocopying, recording, or information storage and retrieval) without permission in writing from RAND.

Published 1998 by RAND
1700 Main Street, PO. Box 2138, Santa Monica, CA 90407-2138
1333 H St., N.W., Washington, D.C. 20005-4707
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information, contact Distribution Services: Telephone: (310) 451-7002; Fax: (310) 451-6915; Internet: order@rand.org
EXPLORING MONEY LAUNDERING VULNERABILITIES THROUGH EMERGING CYBERSPACE TECHNOLOGIES

A CARIBBEAN-BASED EXERCISE

David A. Mussington/Peter A. Wilson/Roger C. Molander

Prepared for the
Office of Science and Technology Policy and the Financial Crimes Enforcement Network

Critical Technologies Institute

RAND
PREFACE

This report summarizes research performed by RAND for the Financial Crimes Enforcement Network (FinCEN) of the U.S. Department of the Treasury. This research was undertaken in concert with the ongoing efforts of the Caribbean Financial Action Task Force (CFATF), and the Commonwealth Secretariat (ComSec) as part of an international effort to examine potential money laundering and financial crime concerns raised by the emergence of Cyberpayments, Internet banking, and Internet gambling systems, particularly as they relate to the Caribbean.

This study was undertaken in recognition that the international community confronts new challenges to traditional oversight of the financial services industry and the investigation of illicit financial activity. The economic growth opportunities flowing from electronic commerce are manifest, as is the international scope of these potential benefits. At the same time, however, the activities of criminals could undermine the promise of this key economic facet of cyberspace. It is important that law enforcement authorities and regulators adapt creatively and flexibly to this emerging electronic commerce environment. Positive and effective responses to the challenges therein are only likely to be achieved through a comprehensive and in-depth analysis of potential avenues of financial abuse and fraud in cyberspace.

This report should be of special interest to those who are exploring the effects of the information revolution on the nature of crime. It should also be of interest to analysts and observers of electronic commerce concerned with the future evolution of regulatory and law enforcement responses to the information revolution.

The purpose of this report and RAND's research was to explore with the public and private sectors, and with international partners, the potential vulnerabilities of Cyberpayments, Internet banking, and Internet gambling to abuse by money launderers and other perpetrators of financial crime. This report is not intended to provide recommendations to either detect or prevent the illicit use of cyberspace-based payment systems. Rather this report outlines the first steps in an emerging international dialogue on the promise and potential problems of cyberspace as an economic environment. Dialogue among the law enforcement and regulatory agencies of different countries will clearly be key to safeguarding the positive potential of the Internet as it expands and matures as a global economic marketplace.

The research reported here was accomplished within the Critical Technologies Institute (CTI). CTI was created in 1991 by an act of Congress. It is a federally funded research and development center operated by RAND. CTI's mission is to:

- Help improve public policy by conducting objective, independent research and analysis to support the Office of Science and Technology Policy in the Executive Office of the President of the United States;
- Help decisionmakers understand the likely consequences of their decisions and choose among alternative policies; and
- Improve understanding in both the public and private sectors of the ways in which technological efforts can better serve national objectives.
CTI research focuses on problems of science and technology policy that involve or affect multiple Executive Branch agencies, different branches of the U.S. Government, or interaction between the U.S. government and states, other nations, or the private sector.

Inquiries regarding CTI or this document may be directed to:
Bruce Don
Director, Critical Technologies Institute
RAND
1333 H Street., N.W.
Washington, D.C. 20005
Phone: (202) 296-5000
Web: http://www.rand.org/cti
Email: cti@rand.org
## CONTENTS

Preface ......................................................... iii
Figures ....................................................... vii
Tables ......................................................... viii
Summary ...................................................... ix
Acknowledgments ........................................... xvi

1. Introduction: Exercise History and Methodology .................. 1
   The Rise of Cyberpayments, Internet Banking and Internet Gambling . 1
   The Purpose of the RAND Effort .................................. 2
   The RAND Exercise ............................................. 3
   Organization ................................................. 6

2. The Current and Future Internet .................................. 7
   Introduction ................................................... 7
   The Internet: An Information Resource .......................... 8
   Internet Growth .............................................. 9
   The Future of the Internet: Infrastructure and Commerce Expansion . 12

3. Cyberpayment Systems ......................................... 14
   Overview ..................................................... 14
   Models of Cyberpayment Systems .............................. 14
   Development in Cyberpayment Systems ........................ 17
   Regulatory and Law Enforcement Issues ........................ 17

4. Internet Banking ............................................ 21
   Overview ..................................................... 21
   Enabling Technologies ........................................ 21
   The Economics of Deployment .................................. 22
   The Special Case of Offshore Internet Banking ............... 23

5. Internet Gambling ............................................. 26
   Overview: Internet Gambling in Context ....................... 26
   Modes of Internet Gambling .................................. 26
   Funds Transfer Vehicles for Internet Gambling ............... 27
   Introduction ..................................................................... 30
   Defining Money Laundering ............................................. 30
   Money Laundering Schemes .............................................. 31
   An Overview of Potential Law Enforcement Responses .......... 34
   Challenge and Response in Retrospect ............................. 36

7. Regulatory, Law Enforcement, and Legal Issues .................. 38
   Introduction: E-Commerce and Government Oversight .......... 38
   Due Diligence .................................................................. 38
   Oversight and Supervision .............................................. 41
   Law Enforcement Issues ................................................ 42
   Legal Issues .................................................................... 43

8. Exercise Findings .......................................................... 45
   Introduction ..................................................................... 45
   Due Diligence Issues ...................................................... 45
   Oversight and Supervision .............................................. 47
   Law Enforcement Issues ................................................ 48
   Legal Issues .................................................................... 49
   Overall Rank Ordered Issue Priorities .............................. 51

9. Conclusions ................................................................... 52
   The Rise of a New Conceptual Model of Cyberspace Criminal Enterprise ............................................. 52
   Type A Failure: The Problem of Jurisdiction in Cyberspace ................................................................. 53
   Type B Failure: The Potential Failure of Traditional Investigative Tools and Techniques ............................. 53
   The Promise of Information Technologies ................................................................. 53
   Implications ..................................................................... 55

APPENDIX A. Exercise Materials .......................................... 57


GLOSSARY ..................................................................... 116
<table>
<thead>
<tr>
<th>FIGURES</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1.1 The Day After Methodology</td>
<td>5</td>
</tr>
<tr>
<td>Figure 2.1 A World Wide Web Page</td>
<td>9</td>
</tr>
<tr>
<td>Figure 2.2 The Expanding Internet – Examples of Domain Names</td>
<td>11</td>
</tr>
<tr>
<td>Figure 3.1 Merchant Issuer Model</td>
<td>15</td>
</tr>
<tr>
<td>Figure 3.2 Bank Issuer Model</td>
<td>15</td>
</tr>
<tr>
<td>Figure 3.3 Non-Bank Issuer Model</td>
<td>16</td>
</tr>
<tr>
<td>Figure 3.4 Peer-to-Peer Model</td>
<td>16</td>
</tr>
<tr>
<td>Figure 3.5 A Hypothetical Example of Potential Cyberpayments Abuse.</td>
<td>19</td>
</tr>
<tr>
<td>Figure 4.1 An Example of Concealed Funds Transfers using Cyberpayment</td>
<td>24</td>
</tr>
<tr>
<td>Figure 6.1 Movement of Funds from the U.S. to Mexico</td>
<td>32</td>
</tr>
<tr>
<td>Figure 6.2 Smartcard-Initiated Movement of Funds to Offshore Bank</td>
<td>33</td>
</tr>
<tr>
<td>Figure 6.3 Internet-Based Funds Movement to an Offshore Location</td>
<td>34</td>
</tr>
</tbody>
</table>
TABLES

Table 1.1  The Exercise Series and Participants ......................... 4
Table 2.1  Internet Trends ............................................. 10
SUMMARY

THE STUDY CONTEXT

This study brought together the interests of three organizations – the Financial Crimes Enforcement Network (FinCEN) of the U.S. Department of the Treasury, the Caribbean Financial Action Task Force (CFATF), a regional body consisting of 25 member nations committed to the prevention of money laundering through monitoring and peer review of internationally recognized anti-money laundering standards, and the Commonwealth Secretariat (ComSec), an inter-governmental organization of 53 member nations and an additional 16 jurisdictions, that supports international cooperation to combat money laundering – in a joint exploration of the effect of the global Internet and other emerging information technology (IT) elements on money laundering and other types of financial crime. In this study effort representatives from over 23 countries came together to discuss potential abuses of emerging Cyberpayment products, Internet banking, and Internet gambling applications. During this process a number of insights were gained, not the least of which was the necessity for continuing interaction and policy work among like-minded countries to address governance issues raised by these three components of electronic commerce.

The principal vehicle used by this study to develop and foster deliberations on the above cited topics was a scenario-based exercise set in 2005. This scenario involved money laundering facilitated principally by a fictitious international financial services and banking, trading, tourism, and gambling conglomerate. The scenario-based approach allowed participants to evaluate the effectiveness of traditional investigative tools and regulatory frameworks projected into the new cyberspace environment.

As presented in the scenario, the potential anonymity of Internet users posed problems for established regulatory and investigative approaches from two related directions. First, customer anonymity means that rules governing the activities of persons or entities initiating Internet-based funds transfers, gambling activities, or Cyberpayments activity may be difficult to enforce. If the identity of a person on the Internet is difficult to authenticate, how can a government know whether its residents are indulging in activities of a proscribed nature in cyberspace? In the absence of information sharing arrangements of some type, such a determination may be difficult, if not impossible. Second, and perhaps more problematically from the point of view of law enforcement, operators of Internet-based financial service companies will be able to offer services across international borders. Whose rules and regulations are to apply to these entities? What rights does the consumer have? Are they governed by his or her locality of residence or by the home jurisdiction of the Internet-based firm? How should the location of an entity’s Internet servers enter into decisions regarding legal and regulatory oversight? What licensing requirements should apply to Internet service providers that facilitate Internet-based financial services? The implications that grows out of both of these concerns created a framework for participants to consider important policy, legal, and law enforcement issues raised by the emergence of electronic commerce.

The study results presented in this report describe one part of a two part process: (1) the design and conduct of the above-cited “RAND exercise” and (2) the generation of a comprehensive list of conclusions and recommendations to guide future policy development work by the CFATF and ComSec. The latter product (provided at Appendix B) emerged as the bottom-line output from a CFATF/ComSec “Workshop on Money Laundering Through
Emerging Cyberspace Technologies” conducted in Trinidad in early May 1998 (with the RAND exercise as its initial component).

PROJECT RESULTS

Participant deliberations in the exercise context yielded a structured set of priorities for future policy development for oversight regimes governing Cyberpayment systems, Internet banking, and Internet gambling. Discussions covered a wide range of topics and problems. An examination of the written records of deliberations yielded a number of important positions and opinions. Examination of group leader reports, recorded group decisions on decisionmaking priorities, and the narrative reports of RAND analysts, yielded a short list of overall issue area priorities:

Legal Issues. Establishing comparable laws and regulations governing cyberspace financial crime.

Oversight and Supervision Issues. Establishing rules governing permissible operators of Internet gambling, Internet banking, and Cyberpayment establishments

Due Diligence/Know Your Customer Issues. Developing international norms for cyberspace “Know Your Customer” measures and procedures.

This list of priorities is indicative of the participants’ consensus that a rule-based approach to the governance of electronic commerce was preferable to an ad hoc implementation of traditional approaches. Within each of four categories, Due Diligence, Oversight and Supervision, Law Enforcement, and Legal, participants considered the appropriate priorities for early action on setting a policy development agenda for like-minded countries to begin coordinated work on appropriate oversight frameworks. Chapter Eight gives a more detailed breakdown of these subsidiary policy development priorities.

In addition to concrete recommendations for coordinated international exploration of policy alternatives, both the exercise design process and the actual exercise deliberations (including the testing phase) fostered education and awareness among many policymakers who may not have had a detailed familiarity with the technologies and systems most fundamental to the Internet and electronic payment systems. In particular, the exercise provided a venue for a broad spectrum of government officials, industry analysts, and academics to come together to reach a shared understanding of the character and immediacy of the cyberspace challenge. While the exercise emphasized the challenges the new technologies, products, and services would pose to established modes of government oversight, participants continually raised the issue of the positive contribution that these developments were expected to bring to regional economies. Balancing the requirements of necessary and effective oversight with the economic imperatives and benefits promised by electronic commerce was a recurring theme in the study effort.

The exercise itself also helped to foster international agreement on an unprecedented set of conclusions and recommendations for beginning work to address the legal, law enforcement, and regulatory treatment of cyberspace and electronic commerce. The deliberations following the RAND-organized exercise period in the May 1998 Trinidad workshop produced a comprehensive list of conclusions and recommendations to guide future policy development work by the CFATF
and Commonwealth Secretariats, in addition to further liaisons between concerned governments and potential electronic commerce product providers (see Appendix B).

**ANALYTICAL ISSUES**

RAND’s analysis of the exercise deliberations yielded a number of important themes and concepts of continuing utility to future analysts and decisionmakers concerned with cyberspace-based payment systems. Our analysis focused on four issues that taken together constitute the central challenge that Cyberpayments, Internet gambling, and Internet banking pose to established governmental modes of oversight. These challenges are (a) the potential rise of a new kind of cyberspace-based criminal enterprise; (b) the potential catastrophic failure of traditional investigative tools and techniques labeled a “Type A Failure”; (c) the problem of jurisdiction in cyberspace, twinned with ambiguities regarding the evidentiary status of electronic data labeled a “Type B Failure”; and (d) the potential promise of information technologies as positive contributors to government oversight, regulatory, and law enforcement capabilities. The next four sections outline each of these subjects in greater detail.

**The Rise of a New Conceptual Model of Cyberspace Criminal Enterprise**

Central to the exercise scenario was a hypothetical international criminal organization able to exploit the technologies of the global information infrastructure (GII) to conceal its activities from government authorities. The organization - the daGama family - used legitimate business activities in banking and financial services, and in the tourism, trading, and gambling industries, operating principally in the Caribbean, to conceal money laundering and narcotics trafficking. While set in a hypothetical future, this criminal organization was itself a direct extrapolation of existing international criminal enterprises. It is a truism among law enforcement authorities that narcotics cartels and other sophisticated organized crime groups are early adopters of advanced technologies. This pattern was earlier indicated by these groups’ adoption of personal computers, pagers, and cellular telephones to facilitate their criminal activities.

With this background, what is one to anticipate regarding potential criminal use of cyberspace? Beyond the current concern with hackers invading private and governmental computing facilities, the emergence of Cyberpayments, the rise of Internet banking, and the emergence of Internet gambling may pose unavoidably attractive targets for criminal exploitation. This reality was explored at length in the exercise scenario, with a number of examples of potential criminal exploitation of electronic commerce products and services outlined in the supporting future history and substantive narratives. Participants uniformly agreed that these means of exploitation would pose significant challenges to their existing arsenal of investigative tools and techniques.

The exercise also conceptualized a hypothetical multinational Western Hemisphere law enforcement and regulatory response to the da Gama family and comparable criminal enterprises - the Permanent Joint Task Force (PJTF). This mechanism was designed to facilitate information sharing, collaborative investigations, and complementary prosecutions. As many participants observed, such a multinational structure possessing operational responsibilities and authorities, does not exist at present anywhere in the world, and would by itself represent a major breakthrough in international governmental cooperation. These same participants also acknowledged, however, that such a response would be insufficient without parallel changes in
national regulatory and law enforcement frameworks governing cyberspace. Clearly, coordinated national and international joint policy development are key to effective oversight.

**Type A Failure: The Problem of Jurisdiction in Cyberspace.** It is possible that, even if law enforcement authorities think that they know "how" a cyberspace crime is being committed, evidence supporting that conclusion may be inadmissible in courts because of a lack of an adequate legal framework. Existing laws appropriate to effective oversight of traditional money laundering, fraud, and financial crime may prove inadequate if they are not adapted — or made adaptable - to keep pace with the new electronic commerce setting.

Controversies regarding the relevant jurisdiction for investigating or prosecuting cyberspace crime may also arise from the fact that electronic commerce is developing much more rapidly than the legal framework that will contain it. In addition, many jurisdictions already lack legislation allowing the use of traditional wiretaps and evidence obtained from wiretaps.

How are states to collaborate in the investigations of cyberspace crime? Existing methods of law enforcement and prosecutorial collaboration will need to be reinforced by the further development of legal and evidentiary rules that allow the introduction and utilization of information derived from computers and the Internet in investigations and subsequent prosecutions. This activity will require that law enforcement and legal authorities gain a greater understanding of the architecture and modes of utilization of the current and future Internet and of potential patterns of abuse that might develop in that environment. Without responsive, collaborative development of these laws criminals could creatively exploit differences in legal regimes to avoid prosecution for cyberspace crime.

**Type B Failure: The Potential Failure of Traditional Investigative Tools and Techniques.** Traditional investigative tools and techniques used by law enforcement to trace money laundering rely on the availability of paper-based records held by regulated financial institutions. These records create a "paper trail" linking an individual to a movement of funds and to potentially useful information or evidence. Anything that interferes with the creation of this paper trail has the potential to seriously impede such law enforcement investigations, perhaps creating a critical gap in evidentiary development.

The Internet, and the associated electronic payment technologies explored in the exercise, have inherent characteristics which create the potential for serious weakening of existing law enforcement tools and techniques. Some examples will help to reinforce this situation: commercially available secure telephones with encrypted communications capabilities may confound established modes of law enforcement wiretaps; the encrypted transmission of financial transactions over the Internet may deny law enforcement its primary traditional means of tracking flows of funds - auditable financial records; Internet gambling applications might employ pseudo-random number generators to "tilt" games in favor of the gambling operator, thereby defrauding players. As an example of the challenge to law enforcement, in the latter case detection of such a fraudulent game could require considerable expertise in computer-based algorithm design, something most law enforcement entities do not possess.

**The Promise of Information Technologies.** On the more positive side, information technologies may offer new capabilities for governments in overseeing electronic commerce and may make unique contributions to the investigation and prosecution of other types of crime. Criminal exploitation of electronic commerce is necessarily rendered more difficult if e-
commerce products and services are "hardened" against fraud and abuse through the deployment of protective tools and techniques. Advanced action by service providers has the potential to reduce fraud on the Internet, thus making law enforcement's job that much more manageable. Three areas of development may make key contributions in this domain: Record Keeping Systems, Authentication Measures, and Tracking Systems.

Record Keeping Systems

Electronic record keeping of commercial transactions on the Internet presents a potentially lucrative data source for law enforcement and governmental regulators. These systems typically collect information on the nature of network traffic, allowing network managers to characterize broad trends in user access. Record keeping systems typically collect their information through the creation of a set of server logs that record the time of an online transaction, the duration of an online session, and information relating to the network address of the consumer or business initiating the transaction. Network logs of this type can underpin more sophisticated analysis of network traffic through a suite of "profiling techniques," whereby artificial intelligence techniques are used to detect patterns of transaction activities associated with money laundering or cyberspace financial crime.

Analysis of network traffic is one quick means of gaining a broad appreciation of the structure and timing of electronic commerce. It allows companies to "narrowcast" their products to particular customers according to their likely interest in purchasing items and creates new information when databases of customer transactions are compared to information from credit reports and online directories. "Data mining" of consumer transactional data is a set of techniques used to find associations between consumer transactional behavior and credit worthiness and other demographic data of interest to marketers. Data mining is performed by statistical software packages installed on high-powered computer work stations. Comparable analytical tools may also be of use to law enforcement authorities and regulators to discern patterns in transactional data associated with criminal activity.

Authentication Measures

Authentication measures allow network operators and government authorities to identify individuals or entities involved in cyberspace-based financial activity. A number of technologies are key to this capability:

Digital Signatures - a label attached to e-mail, data, or electronic value flowing within a network that authenticates the identities of particular individuals or entities. When tied to particular transactions, digital signatures create an electronic trail, linking online transactions with particular individuals.

Biometric Forms of Identification - hardware and software systems that authenticate the identities of human beings through the electronic capture of unique data characterizing a person's features. Examples include images of a person's fingerprint or palm print, a laser-scan of an individual's retina or iris, and a voiceprint.

The combination of record keeping systems and authentication measures could yield an infrastructure of potentially great utility to law enforcement and government regulators in establishing the money/illicit activity nexus so important to the building of a case for potential prosecution.
Tracking Systems

Network tracking systems are, perhaps, the most experimental of all the techniques becoming available for conducting surveillance over online activities. Still in research are techniques deriving from already deployed artificial intelligence (AI) applications that use knowledge-based systems to characterize network traffic according to such criteria as point of origin, duration of online session, and identity of the user. The major difference with these techniques is that they are implemented in software analogous to that of a computer virus.

Network-borne tracking systems are of two broad types: classifier systems, using rule-based models derived from the judgement of human experts to categorize online traffic; and software agents with elementary machine “learning” capabilities that are reinforced by continual exposure to transaction data in a network setting.

Each of these tools has the potential to conduct partially or completely autonomous data-gathering activities - in some sense analogous to motion or temperature sensors in the physical world. Development of these tools is at the speculative “outer edge” of research, and their true potential for intercepting potentially suspicious electronic commerce activity remains to be demonstrated.

Electronic traces of online activity raise concerns regarding consumer privacy and potentially inappropriate uses of sensitive information by unauthorized persons. It is important then to consider these techniques in relation to the regulatory and law enforcement purposes they may support. It is nonetheless true that the electronic infrastructure to perform many of these activities will likely emerge as a consequence of the growth of electronic commerce.

Entities providing funds, goods, and services over the net are necessarily concerned with ensuring the safety and security of their transaction systems from compromise by hackers or thieves. In turn, network providers of financial services must meet established safety and soundness concerns relating to their ability to identify customers. Each of these concerns means that some sort of authentication, tracking, and record-keeping infrastructure will likely emerge from the electronic commerce arena as a result of market forces.

IMPLICATIONS

Taken together, the challenges described above raise many questions regarding the continuing ability of governments to maintain, and/or sustain progress toward existing anti-money laundering and anti-financial crime objectives. Existing institutions simply are not yet designed to manage emerging cyberspace technologies or respond to the potentially serious impact these systems could have on the investigation and prosecution of organized crime.

A coordinated international response to the full spectrum of these problems seems an appropriate place to begin. Crafting and successfully marketing such a strategy to protect the security and integrity of cyberspace-based financial activity now and in the twenty-first century should be an imperative of all those interested in the growth of this new medium.
The results of the CFATF/ComSec workshop on Money Laundering Through Emerging Cyberspace Technologies (Appendix B) represent an important step - the first structured international attempt to come to grips with this complex set of challenges. Moving forward with policy development initiatives would provide concrete evidence of a serious international effort in this new arena. It would also provide an opportunity to exploit the emerging international consensus that cyberspace be taken seriously as both a technological challenge, and a legal, administrative, and cultural challenge to traditional modes of economic and regulatory governance.
ACKNOWLEDGMENTS

We are grateful for the contributions of many people within FinCEN, the Department of Treasury, the CFATF Secretariat, the Commonwealth Secretariat, and representatives of CFATF member states for their invaluable assistance in the conception and carrying out of this project. In particular, we would like to thank Carlos Correa, Executive Director of CFATF, Diane Stafford of the ComSec, and Shaun Lonergan, Gary Novis, and Michelle Gideon of FinCEN for their contributions throughout the project.

Special thanks must also go to our secretary and assistant Darlette Gayle who maintained high levels of competence and good humor through countless exercise drafts and attendee lists. Thanks also to our RAND colleagues Anna Slomovic and Robert H. Anderson for their very constructive reviews of the draft report.

We would especially like to express our appreciation for those who represented the following governments, agencies, and international organizations at the January, February and March 1998 exercise tests, and at the April 6/7 and May 5 formal exercises:

<table>
<thead>
<tr>
<th>Country</th>
<th>Office</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anguilla</td>
<td>Office of the Attorney General</td>
</tr>
<tr>
<td></td>
<td>Ministry of Finance</td>
</tr>
<tr>
<td>Antigua</td>
<td>Royal Antigua Police Force</td>
</tr>
<tr>
<td>Aruba</td>
<td>Unusual Transactions Reporting Office (MOT)</td>
</tr>
</tbody>
</table>
| Australia            | Transaction Reports & Analysis Center (AUSTRA)
| Bahamas              | Office of the Attorney General            |
| Barbados             | Office of the Attorney General            |
|                      | Department of Public Prosecutions         |
|                      | Office of the Solicitor General           |
| Belize               | Central Bank of Belize                    |
| Bermuda              | Office of the Attorney General            |
|                      | Ministry of Finance                       |
| British Virgin Islands| Financial Services Department             |
| Canada               | Royal Canadian Mounted Police             |
| Cayman Islands       | Office of the Financial Secretary         |
|                      | Ministry of Legal Affairs                 |
|                      | Monetary Authority                        |
| Costa Rica           | Drugs Control Police                      |
| Dominica             | Office of the Attorney General            |
|                      | Department of Public Prosecutions         |
| France               | Regional Crime Squad                      |
| Grenada              | Office of Public Prosecutions             |
|                      | Police Force                              |
| Jamaica              | Constitutional Reform Unit                |

xvi
Montserrat
Ministry of Finance

Netherlands Antilles
Bank van de Nederlandse Antillen

Panama
National Banking Commission

St. Kitts & Nevis
Office of the Attorney General
Royal St. Kitts & Nevis Police Force

St. Lucia
Ministry of Legal Affairs
Office of Public Prosecutions
Financial Services Department

St. Vincent & the Grenadines
Office of the Attorney General

Trinidad & Tobago
Ministry of National Security
Office of the Attorney General
Strategic Services Agency
Counter Drug Crime Task Force
Central Bank of Trinidad and Tobago

Turks & Caicos
Financial Services Commission

United States
U.S. Department of Treasury, FinCEN
U.S. Customs Service
IRS
Drug Enforcement Administration
U.S. Attorney’s Office, Southern District of New York (SDNY)
Office of the Comptroller of the Currency
Federal Reserve System
Federal Deposit Insurance Corporation

Multi-national Organizations
Caribbean Commission (CARACOM)
Caribbean Financial Action Task Force
Commonwealth Secretariat (ComSec)
Eastern Caribbean Central Bank (ECCB)
European Commission, Drugs Control Office
U.N. Global Program Against Money Laundering

Industry
Citibank (N.A.)
Claymen & Rosenberg
KPMG Peat Marwick
Lionel, Sawyer & Collins
Mondex International
NationsBank
Security First Network Bank
Spectrum Trading Group
SunTrust Bank
1. INTRODUCTION: EXERCISE HISTORY AND METHODOLOGY

The rise of electronic commerce carries with it a number of positive benefits. This in turn has provided the incentive for the introduction and development of a wide array of related new payment technologies, such as Internet banking, smart cards, and digital money. The expansion of the Internet is bringing hopes of new economic opportunities and dreams of new wealth for many entrepreneurs. The spread of high-capacity telecommunications and computing connectivity to new parts of the world is creating a truly global electronic marketplace where consumers and service providers will be able to interact. Governance of the new environment is in flux, as traditional national regulatory and legal regimes governing commerce, gambling (where legal), and financial service providers are challenged by the new environment.

The Commonwealth Secretariat, as a result of an August 1997 meeting of Law Officers and Ministers of Legal Affairs of Small Commonwealth Jurisdictions, expressed their concern over increased potential money laundering through cyberpayment/Internet systems in general, and Internet gambling in particular. The Ministers therefore called on the Commonwealth Secretariat to seek to influence the development of a multilateral response to these activities. Concurrently, as a result of the CFATF “Casino Regulatory Conference: Money Laundering Risks,” in June of 1997, the CFATF became aware of the significant role that the Caribbean was performing in the field of Internet gambling, both in the development of gambling software and in hosting Internet gambling sites. Therefore, the CFATF in its October 1997 Ministerial meeting approved a work plan designed to enhance the understanding of these issues by CFATF member governments.

The CFATF and Commonwealth Secretariats agreed to conduct a workshop in the Caribbean to explore these issues. The Secretariats approached the U.S. Department of the Treasury’s Financial Crimes Enforcement Network (FinCEN) for technical assistance and to co-sponsor a “Money Laundering through Emerging Cyberspace Technologies” exercise in May of 1998.

Internationally, Cyberpayments has already received appreciable attention. Multilateral discussions and studies have been undertaken by the G-7 Financial Action Task Force, the G-8 Subgroup on High Tech Crime, and the G-10 Working Party on Electronic Money. In June of 1996 a new recommendation 13 was added to the FATF’s 40 Recommendations. It states that “countries should pay special attention to money-laundering threats inherent in new or developing technologies that may favor anonymity, and [they should] take measures, if needed, to prevent their use in money laundering schemes.” CFATF observations on the same topic formed the backdrop for the exercise.

THE RISE OF CYBERPAYMENTS, INTERNET BANKING, AND INTERNET GAMBLING

CFATF Member governments have developed legislation governing banking and other financial services and, where appropriate, gambling and/or other gaming activities. Electronic
payment products have only recently become the object of regulatory treatment. The trans-border features of the Internet mean that gambling and financial service products delivered over the network may not be adequately regulated by traditional means.

Credit and debit cards are two well understood traditional payment instruments used by customers around the world. Both of these instruments share an important feature - they are issued by an entity operating under the laws and financial oversight rules of a particular locality. More narrowly, credit and debit cards, alongside gambling activities, involve the close regulation of a business entity that delivers a regulated package of services - again under the oversight of a government. On a more technical level, both of these products also employ network-based authorization for transactions utilizing consumer credit or debit accounts.

Whereas the operations of debit and credit cards are well understood, e-cash products break this well understood authorization nexus, whereby in the absence of a regulated third party (e.g., a bank) direct electronic transfers of funds on a peer to peer basis become possible. Internet banks, and electronic commerce more broadly, open the way toward a partial disintermediation of the payment system - whereby in the absence of a regulated third party (i.e., a bank) electronic transfers of financial value between two or more entities will be enabled.

In particular, the empowerment of individuals to transfer electronic cash - and to gamble with these funds with establishments in a foreign jurisdiction - significantly increases potential profits available to the operators of Internet businesses. In effect, economic competitiveness and efficiency motivations are fostering an expansion in networks and creating an infrastructure for new products and services previously unavailable to consumers - and potentially beyond the reach of traditional regulatory efforts.

The international character of Internet banking, Internet gambling, and Cyberpayments probably makes joint international action almost certainly essential to countering potential abuse of electronic commerce. The exercise described in this report sought to address shared international dilemmas in the crafting of both the scenario narrative and the deliberative materials.

THE PURPOSE OF THE RAND EFFORT

The goal of this research effort is to explore the dimensions and implications of potential future illicit use of Cyberpayment, Internet banking, and Internet gambling products by money launderers and others seeking to illegally conceal funds from governmental authorities. This research is also intended to identify - at least in a preliminary fashion - possible medium-term priorities for further work in the direction of crafting law enforcement and regulatory responses to potential patterns of electronic commerce abuse.

The application of new information technologies to the emerging electronic commerce arena is still in its earliest phase. The future of electronic commerce will depend on its ability to compete with traditional commercial activities for customers, on the further development of its underlying Internet and encryption technologies, and on the emergence of legal and regulatory regimes able to ensure against significant patterns of abuse. Developments in each of these areas are likely to mature in the next few years as cyberspace emerges from its "early adopter" phase. For these reasons, law enforcement and regulators in many countries should work closely with private sector electronic commerce entities to better understand the range of systems and products that governments must oversee.
Cyberpayment product providers have already begun a dialogue with various government entities in an effort to secure these products from potential criminal abuse. In this atmosphere of goodwill, government and the private sector share a real opportunity to design anti-abuse elements into the systems and products constituting the electronic commerce universe. As governments and the private sector collaborate on minimizing potential abuses, a continuing dialogue between the two will undoubtedly foster greater transparency on patterns of criminal misuse and greater speed in applying potential remedial law enforcement measures.

The RAND research effort described in this report was designed to support these objectives.

THE RAND EXERCISE

To address CFATF, ComSec, and FinCEN concerns in this area, RAND designed, conducted, and analyzed a strategic decisionmaking exercise directed at both the potential problems and the potential opportunities that the emergence of electronic commerce poses for international anti-money laundering and anti-financial crime efforts.

To accomplish the project's research goals, the exercise sought to achieve three primary goals:

1. Explore dimensions and implications of potential future illicit use of Cyberpayments, Internet banking, and Internet gambling by money launderers

2. Identify key potential or generic vulnerabilities associated with such activities

3. Facilitate the formulation and development of recommendations for:

   - government/industry cooperation
   - regulatory, law enforcement and legal responses
   - international and regional cooperation among participating governments.

Participants in the test series (see Table 1.1) and the final exercises included representatives of CFATF member governments; officials from international organizations; individuals from the Cyberpayment, Internet banking, and Internet gambling industries; and academic analysts. Responses to potential abuse in each of the three sub-categories were compiled through recording the exercise experiences of participants and through observation and analysis of dilemmas posed by the exercise itself. During this process, traditional law enforcement and regulatory measures were evaluated in the light of the potential challenges posed by electronic commerce technologies. Extensive testing of the exercise materials during a lengthy test sequence helped to refine the questions and issues that structured the exercise.

To make the exercise environment as familiar to participants as possible, a scenario was designed involving issues of importance to current decisionmakers and analysts - even though these were transformed through an exploration of possible avenues of criminal abuse of new cyberspace-based payment technologies. The scenario framework included a narcotics cartel and an international financial services and banking, trading, gambling, and tourism conglomerate
involved in money laundering. The scenario was set in 2005, in order that the technologies underlying electronic commerce could plausibly be deemed fully mature.

<table>
<thead>
<tr>
<th>DATE</th>
<th>LOCATION</th>
<th>EVENT/PARTICIPANTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>23 January 1998</td>
<td>Washington D.C.</td>
<td>Test: RAND and FinCEN staff, CFATF member nation representatives</td>
</tr>
<tr>
<td>20 February 1998</td>
<td>Washington D.C.</td>
<td>Test: RAND and FinCEN staff, CFATF member nation representatives</td>
</tr>
<tr>
<td>20 March 1998</td>
<td>Miami, FL.</td>
<td>Test: RAND and FinCEN staff, CFATF member nation representatives</td>
</tr>
<tr>
<td>6/7 April 1998</td>
<td>Barbados, W.I.</td>
<td>Dry Run: RAND and FinCEN staff, CFATF member nation representatives</td>
</tr>
<tr>
<td>5/6 May 1998</td>
<td>Trinidad and Tobago</td>
<td>Operational Exercise: Senior CFATF member nation representatives</td>
</tr>
</tbody>
</table>

Table 1.1 - Exercise Series and Participants

In support of the scenario a “future history” was developed that described (1) hypothetical product features and developments in the Cyberpayments, Internet gambling, and Internet banking industries; (2) the emergence of an financial services and banking, international tourism, trading, and gambling conglomerate; and (3) international law enforcement and regulatory responses to perceived e-commerce abuse.

The Exercise Methodology consisted of three steps (see Figure 1.1 below):

In STEP ONE participants are introduced to a looming scenario where the task is to come to grips with a worsening situation and make recommendations to a senior decisionmaker. STEP TWO presents exercise participants with a steeply worsening crisis, and with a series of events that appear relatively unresponsive to policymaker choices. This step’s activities resemble those of STEP ONE. STEP THREE is a “lessons learned” phase of the exercise. In this step participants return to the near future, where their task was to evaluate and rank order issues and problems important to the more effective resolution of STEP ONE and STEP TWO dilemmas.
Exercise Methodology

Figure 1.1 - The Day After Methodology

The exercise scenario involved a simulated top-level advisory group where participants served as senior advisors to a decisionmaking body. The events of the scenario served as the backdrop for consideration of dilemmas and controversy integral to international legal and law enforcement treatment of potential abuse of Cyberpayments, Internet banking, and Internet gambling applications.

The scenario posited a fictional international business conglomerate that was highly successful in facilitating money laundering for narcotics traffickers and other organized crime groups. The fictional company used Cyberpayments, Internet banking, and Internet gambling to conceal its activities from jurisdictions likely to pursue prosecutions. In this environment, concerned governments from the Western Hemisphere decided to investigate and prosecute the company as a money laundering enterprise.

The May 5-6 RAND exercise was the first component of a CFATF/ComSec workshop on Money Laundering through Emerging Cyberspace Technologies. The second component of that workshop was essentially a deliberation of policy initiatives involving Caribbean, North American, and European governmental participants.

---

2 The "Day After" methodology has been used to examine a number of other policy problems characterized by a high technology component. See Roger C. Molander, David A. Mussington, and Peter Wilson, Cyberpayments and Money Laundering: Problems and Promise (Santa Monica, CA: RAND), MR-965-CTI 1998; and, Roger Molander, Peter Wilson, and Andrew Riddile, Strategic Information Warfare: A New Face of War (Santa Monica, CA: RAND, 1996) MR-661-OSD 1996.
Representatives met as a group to deliberate on priority issues for policy development in the governance of Cyberpayments, Internet banking, and Internet gambling. This deliberative phase was critically informed and enabled by the broader consideration of electronic commerce issues provided by Steps One through Three. The nominal “Step Four” of these activities concentrated on the Caribbean context of electronic commerce governance.

ORGANIZATION

The remaining chapters of this report are organized as follows. Chapter Two describes the structure and makeup of the current Internet and offers some conjectures about the future of the cyberspace environment. Chapters Three, Four, and Five offer capsule discussions of the Cyberpayments, Internet banking, and Internet gambling industries. Chapter Six introduces potential patterns of criminal abuse of the emerging electronic commerce environment and summarizes some initial technical responses designed to secure cyberspace from criminal abuse. Chapter Seven presents Regulatory, Law Enforcement, and Legal Issues. Chapter Eight presents the findings of the exercise. Chapter Nine presents RAND’s conclusions regarding general lessons from the exercise experience and draws out underlying themes of likely significance to governmental oversight of electronic commerce. The appendices present the exercise materials employed during the project in their final form as used in the Trinidad workshop.
2. THE CURRENT AND FUTURE INTERNET

INTRODUCTION

The Internet is the basic environment enabling innovations in electronic commerce in general, and new payment technologies in particular. The Internet itself is a “network of networks” linking regional networks through a common communications protocol or language. Beyond this simple definition, the Internet constitutes an interconnected set of telecommunications and computing resources. These resources are owned by public (governmental) agencies and by private sector commercial entities.

Most basic to the structure of the Internet is the public switched telephone network. Because of the ubiquity of telephone connectivity in advanced industrial societies, computers connected to that network can exchange both data and shared control over geographically dispersed facilities.

The telephone network links persons (or computers) on the public switched network. In order for this network to be used for computer-to-computer communication a particular language - or set of communications protocols - had to be designed. This set of protocols - the Transport Control Protocol/Internet Protocol suite (TCP/IP) are the result of a US government research project undertaken under the auspices of the Defense Advanced Research Projects Agency (DARPA) in 1969.\footnote{1} Successful development of this common framework of inter-computer communication led to the establishment of the ARPANET - a precursor of the current Internet - as a platform for both conducting and facilitating military communications research. ARPANET was designed to be resistant to partial outages and to have decentralized administration. The modern Internet inherited both of these features. Each is important enough to warrant separate treatment.

Resistance to Outages

This feature of the Internet derives from the packet-switched architecture of this computing/communications system. In brief, messages passing over the Internet are broken up into discrete packets containing basic identifying information in a packet-header and a so-called data block.

The packet header contains information giving the point of origin of the message, its data type and authorship, and its ultimate intended destination. When a message is sent, it passes through a set of routers that direct it forward depending on a reading of the header information in each packet. Because routers are often geographically separated (as on the global Internet), no single router malfunction or outage can prevent a message from proceeding to its ultimate destination. Rather, routers upstream (logically prior to the disrupted router) will divert packets around the fault - altering the route followed by packet traffic and ensuring its ultimate delivery.\footnote{2} Routers are connected to multiple other routers, so that many different paths exist between a message’s point of origin and its destination. These routers repeatedly test each other’s status; when one responds inappropriately, packets are diverted to alternative routers.\footnote{3}

\footnote{3} The authors would like to thank Robert Anderson for clarifying the operation of routers on the Internet.
A large network with these characteristics is very resistant to single-point failure. In turn, the inherent architecture of a TCP/IP network means that predicting the particular path that a packet will travel between its origin and its ultimate destination is practically impossible, a fact with significant implications for the administration of networks.

Decentralized Administration

This feature of TCP/IP networks derives from the semi-independent operation of routers and network access points (NAPs) through which traffic is managed. Decentralized administration is thus an inherent feature of a network designed to be resistant to partial outages in this fashion.

The administration of the Internet is not entirely decentralized, however. As is made clear below, a small set of root directories identifying the owners and logical locations of particular Internet Protocol (IP) addresses is necessary for the efficient functioning of the network. As the geographical scope of the Internet expands, the number of servers containing this central (or “root”) directory will also increase.

Another feature of the Internet that reinforces “physical” decentralized administration is the overlapping set of organizations that coordinate the technical and operational standards facilitating Internet growth. Because the governance framework is in transition, it is fair to say that there are important ongoing controversies regarding administration and technological standards on the Internet. Their outcomes will almost certainly carry significant political and economic repercussions. The structure and makeup of this complex of organizations are described later in this chapter.

THE INTERNET: AN INFORMATION RESOURCE

Most users interact with the Internet as a basic information utility. In this sense the Internet resembles a telephone company or an electrical utility by delivering basic services to a geographically distributed user base. As an information resource it provides access to widely distributed information repositories analogous to public libraries. Of course, fee-paying services can also be accessed over the Internet. These services, and their regulation, are among the most controversial of issues confronting government and society in the emergence of cyberspace.

In 1986, the National Science Foundation (NSF) upgraded the prior collection of network links with the establishment of the Internet backbone - a high-speed network linking disparate regional networks made up of university computing facilities and supercomputer research centers. Since then high-speed links between regional networks have grown and become increasingly privatized, with MCI, Sprint, and AT&T all providing high-speed communications links that carry Internet-based data traffic.

---

Prominent Internet Applications

The predominant applications on the Internet are the World Wide Web (WWW), electronic mail (e-mail), Telnet (remote login) applications, and the File Transfer Protocol (FTP). The most utilized application on the Internet is e-mail.\(^6\) The World Wide Web - a graphical user interface into the information available on the Internet - is the application that generated the acceptance as an information appliance.

As Figure 2.1 makes clear, visual and textual information are both made available on the World Wide Web. In turn, both video and audio applications are being introduced that threaten to undermine currently dominant television and radio forms of entertainment and news delivery.\(^7\) Telnet and FTP represent applications enabling remote login and administration of computing facilities, and bulk file transfers across the Internet, respectively. These applications are critical to information retrieval and communication.

INTERNET GROWTH

The Internet is growing at an accelerating rate. From its origins in 1969, the Internet remained predominantly an academic and military research environment until the late 1980s. Growth during this period was relatively slow, allowing for the consolidation of technical standards in the TCP/IP and HTML (hypertext markup language) areas. Since 1990, however, the spread of the Internet has accelerated rapidly as the user base began to spread beyond the academic realm.


\(^7\) See [www.RealAudio.com](http://www.RealAudio.com) for details on the dominant Internet real-time audio and video applications.
As Internet growth gains more public attention, demands for better metrics, and measurement of its "size" are likely to increase. Network Wizards, one of the most highly regarded sources of statistics on the size and growth of Internet connectivity has revised its own prior estimates of the rate of Internet growth upward substantially on the basis of improved sampling methods.\(^8\)

<table>
<thead>
<tr>
<th>Internet Trends</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>December 1995</strong></td>
</tr>
<tr>
<td>- 14 Million Computer Hosts</td>
</tr>
<tr>
<td>- 40 Million Internet Users</td>
</tr>
<tr>
<td>- 1 Billion E-Mail Messages Per Month</td>
</tr>
<tr>
<td><strong>December 1996</strong></td>
</tr>
<tr>
<td>- 21 Million Computer Hosts</td>
</tr>
<tr>
<td>- 63 Million Internet Users</td>
</tr>
<tr>
<td>- 1.5 Billion E-Mail Messages Per Month</td>
</tr>
<tr>
<td><strong>January 1998</strong></td>
</tr>
<tr>
<td>- 29 Million Computer Hosts</td>
</tr>
<tr>
<td>- 80 Million Internet Users</td>
</tr>
<tr>
<td>- 2.5 Billion E-Mail Messages Per Month</td>
</tr>
</tbody>
</table>

Table 2.1 - Internet Trends\(^9\)

Trends regarding the Internet can also be expressed in terms of the number of users regularly interacting with e-mail or World Wide Web applications. Estimates of Internet growth combining figures from the U.S. Department of Commerce and those of the U.S. Department of the Treasury are shown above.

The global nature of the Internet is nowhere more exemplified than by the domain name system - the central directory assigning names to host computers connected to the global network. Two types of domains exist, country code top level domains (ccTLDs), and generic top level domains (gTLDs).

Members of the first group, ccTLDs, are assigned by a national naming authority in a particular country. Examples of these domains include the .us, uk, and .ca name spaces. In the United States, the .us domain is used mostly by state and local governments. Other countries have differing methods of assigning use of their sovereign domain space.

---


The most widely used domains are the gTLDs, examples of which are .com, .org, .net, and .edu. A second set of gTLDs is reserved for U.S. government use. These domains are .mil and .gov, with .int reserved for international organizations. As Figure 2.2 illustrates, the domain name system is truly global, with both developed and developing countries - and their private sector entities - establishing an Internet presence at an accelerating rate.

The Internet Today

![Image of the world with various country codes and domain name system examples]

Figure 2.2. The Expanding Internet – Examples of Domain Names

The coordination of the Internet takes place through a grouping of public and private entities. Administration of the domain name system and the Internet Protocol (IP) address system (numerical addresses of computers, analogous to telephone numbers in the public telephone system) is done by the InterNIC consortium, operated for the US National Science Foundation by a private company, Network Solutions Inc, and the Internet Assigned Numbers Authority (IANA), a body run by Professor John Postel at USC.\(^\text{10}\) A number of other organizations are also involved in administering the Internet.\(^\text{11}\) Among these are:

**Internic** - The domain name registry operated for the U.S. National Science Foundation by Network Solutions, Inc. of Herndon, Virginia. The domain registry is a directory of Internet domains – or names – assigned to entities with an Internet presence.

---

\(^{10}\) Jon Postel, the IANA chair, is a professor of Computer Science at the USC Information Sciences Institute.

\(^{11}\) It should be noted that the roles and responsibilities of these entities are now being allocated to a yet to be established non-profit corporation with global representation on its governing board. The exact makeup and content of the new group's mandate has yet to be decided.
The World Wide Web Consortium – This consortium is made up of commercial and non-profit entities involved in the design and implementation of technical standards on the Internet.

Regional Internet Registries – These registries allocate discrete subsets of the Internet protocol address space to private and public entities in different parts of the world.

The Internet Engineering Task Force – The task force that implements technical standards in the routing and switching hardware through which Internet traffic is transmitted.

The Internet Engineering Steering Group – The group charged with designing technical standards and Internet architecture studies for the future of wide bandwidth networks.

The Internet Architecture Board – A board made up of governmental, academic, and business technical experts who define standards for the Internet’s data traffic and switching systems.

THE FUTURE OF THE INTERNET: INFRASTRUCTURE AND COMMERCE EXPANSION

The future of the Internet is likely to see a further geographic expansion in connectivity to the few areas of the world not currently touched by network services. In turn, new delivery media will likely be added to the Internet suite of technologies with smart cards, database management technologies, and artificial intelligence products merging with TCP/IP networks.

An additional change in the Internet infrastructure will come from the increasing interconnection among cellular, satellite-cellular, and fiber optics communications infrastructures. The emergence of these systems will greatly increase the speed of the Internet, further expanding the scope and quality of service and information products available to users.

Lastly, some form of strong encryption is likely to be deployed in order to protect electronic commerce applications. The transmission of funds and other sensitive data “in the clear” on the Internet poses clear risks to funds safety and consumer privacy. Encryption and other computer security techniques are being added to the basic Internet in order to secure it from potential abuse and to serve as a platform for the further migration of many “real life” information services into cyberspace.

The growth of commerce on the Internet is itself a result of progress in business to business electronic commerce relationships which have fostered purchasing and information transfer standards. Much of this growth is largely invisible – embedded as it is in the distribution infrastructure characterizing many traditional sectors of the macroeconomy.

---

13 In fact, a recent decision by the Department of State allows financial institutions to utilize 128-bit encryption in their funds transfer systems (versus an upper limit of 56 bit encryption key lengths on exported encryption products), so long as they file a key recovery plan with the appropriate U.S. government regulatory agencies.
14 The controversy over encryption policy is, of course, ongoing. For an overview of US Government attempts to craft an encryption policy, see Bruce Schneier and David Banisar, The Electronic Privacy Papers (New York: John Wiley & Sons, 1997).
15 Frances Cairncross, The Death of Distance, p. 146.
Reforms in inventory control, online ordering of spare parts, and the establishment of intranets linking manufacturers with their principal suppliers, all help to create a pattern of electronic commerce standards and partnerships. These relationships also allow for the standardization of contracts, electronic payment and settlement arrangements, and goods delivery procedures. That these developments are taking place while the Internet is still in an embryonic state is indicative of the explosive efficiency and speed benefits that electronic commerce provides to users.\textsuperscript{17}

The continued growth and integration of the global Internet will also likely lead to the increased interoperability and integration of emerging cyberpayment, Internet banking, and Internet gambling services – a subject addressed at greater length in the next three chapters.

3. CYBERPAYMENT SYSTEMS

OVERVIEW

A number of different types of Cyberpayment systems are currently under development, testing, and in consumer trials. Two general types are dominant and are extensively cited in the exercise materials: Stored value-type smart cards and Internet-based payment systems (e.g., electronic cash, or “e-cash”). Recently these two technologies have begun to converge as interoperability agreements between e-cash and smart card developers create a single Cyberpayment infrastructure with a variety of electronic payment systems.

Progress toward technical and commercial standards, while occurring, is moving forward quite slowly. Full financial interoperability - involving clearing and settlement - may prove extremely difficult, especially in an increasingly varied international environment. Differences in financial liability in international jurisdictions - with varying impact on issuing institutions - mean that system level controls may emerge on the international scene that impede interoperability or product utilization.

Some Cyberpayment instrument features, such as peer-to-peer value transfer and partial payer anonymity, offer consumers an instrument with much of the flexibility and convenience of cash, together with an enhanced ability to conduct purchases (of physical and information goods and services) on an almost global basis. As a consequence, government authorities may face an environment in which the use of physical currency has been substantially reduced by the easy availability of widely accepted Cyberpayment equivalents.

Four discrete kinds of cyberpayment instruments are present in the market place at present. The next section offers a capsule summary of their key features.

MODELS OF CYBERPAYMENT SYSTEMS

1. **The Merchant Issuer Model (Figure 3.1).** Smart card issuer and seller of goods are the same. Example: the Creative Star farecard used by riders of the Hong Kong transit system.
2. **The Bank Issuer Model (Figure 3.2).** Merchant and smart card issuer are different parties. Transactions are cleared through traditional financial systems. Examples: Banksys’ Proton card in Belgium (now licensed by American Express) and the Danmont card in Denmark.
3. **Non-Bank Issuer Model (Figure 3.3).** Users buy electronic cash from issuers using traditional money and spend the electronic cash at participating merchants. Issuer subsequently redeems the electronic cash from the merchant. Example: CyberCash’s electronic coin product.
4. **Peer-to-Peer Model (Figure 3.4).** Bank or non-bank issued electronic cash is transferable between users. Only point of contact between the traditional payments system and electronic cash is the initial purchase of electronic cash from the issuer and redemption of electronic cash from individuals or merchants. Example: Peer-to-Peer value transfers through the MONDEX stored value smart card.

The four models allow value to be added to or transferred from stored value-type smart cards using a variety of vehicles.
Figure 3.1. Merchant Issuer Model

Figure 3.2. Bank Issuer Model
Figure 3.3. Non-Bank Issuer Model

Figure 3.4. Peer-to-Peer Model
DEVELOPMENTS IN CYBERPAYMENT SYSTEMS

A number of Cyberpayment system pilots have been launched in different parts of the world. (In general, bank and credit card consortia have created joint ventures to test consumer acceptance of these new payment instruments.) Some believe that stored value-type smart cards and Internet-based payments products will develop and be accepted quickly creating a Cyberpayment infrastructure with varying characteristics and a number of different electronic payment products. Others believe, given the growing success of debit cards and other more conventional payment methods, that this process will be much more prolonged.

The material that follows describes some recent stored value smart card and Internet-based payment system initiatives.

One well-known pilot program is the MONDEX stored value smart card which is being tested in the U.K., Canada, the U.S., Hong Kong, New Zealand, and Australia. In November of 1996, MasterCard International purchased 51 per cent of MONDEX International; and in December of 1996 seven major US corporations joined together to establish MONDEX USA, a firm designed to commercially develop and implement the MONDEX electronic cash system in the US. Participating corporations in the MONDEX USA venture are: Wells Fargo, MasterCard, AT&T Universal card Services, Discover card, Michigan National Bank, Chase Manhattan Bank, and First Chicago. In September of 1996, MONDEX International signed a joint development agreement with CyberCash (an Internet-based payment system provider - see below) to integrate MONDEX’s stored value smart card technology with CyberCash’s electronic wallet. In July of 1998 Cybercash announced an agreement to merge with another provider of Internet-based financial services, First Virtual Holdings.

American Express will use Proton Electronic Purse technology to implement multiple stored value smart card pilots over the next few years. Proton (owned by BANKSYS) is already being either piloted or rolled out in Canada, Australia, Sweden, Belgium, Brazil, the Netherlands and Switzerland. In July of 1998 Visa International joined American Express and its partners in the creation of Proton World International, a joint venture providing smart card services and payment products to the financial services industry.

In March of 1998 Visa International announced the roll-out of its VisaCash smart card product. This announcement consisted of the release of the smart card platform to member financial institutions, who would then make decisions regarding the appropriate role of smart cards in their retail financial products. Visa is currently active in over 70 pilot smart card programs in 30 countries.

REGULATORY AND LAW ENFORCEMENT ISSUES

Analysis of Cyberpayments’ impact on payment systems typically emphasizes five key features: (1) Disintermediation; (2) Bank or Non-bank Issuance; (3) Peer-to-Peer Transfers; (4) Transaction Anonymity; and (5) Denomination Limits and Expiration Dates. Each of these basic features is described in more detail below. While some of these features make Cyberpayments attractive as a potential means to reduce transaction costs in commerce and contribute to the increased efficiency of the economy, they are also consistent with vulnerabilities that may be exploited by criminals.

Disintermediation. Historically, law enforcement and regulatory officials have relied on the intermediation of banks and other regulated financial institutions to provide “choke points”
through which funds must generally pass and where records would be maintained. Disintermediation involves the transfer of financial value between entities without the intermediate involvement of an identifiable third party subject to governmental oversight (e.g., record-keeping requirements via a bank). Should Cyberpayment systems permit disintermediated value transfers in unlimited amounts, money launderers could use this as an opportunity to avoid traditional law enforcement money-tracing methods.

A Variety of New Cyberpayment Providers. Banks and new issuers of electronic payment instruments may be subject to different rules regarding their operation of Cyberpayment systems. This difference is already the case in several nations where non-bank Cyberpayment issuers are currently subject to a set of rules different from that of banks. A simple extension of traditional payment system oversight to new non-bank Cyberpayment issuers may address some of the concerns regarding potential system abuse. However, the new systems are configured differently and are constantly mutating, so a “one size fits all” regulatory approach is not necessarily appropriate or even possible.

Peer-To-Peer Transfer Capabilities. Some Cyberpayment systems allow consumers to transfer value peer-to-peer (and thus, disintermediated), using an electronic “wallet,” a telephone, or the Internet. Such value transfers pose perhaps the most direct challenge to governmental oversight of Cyberpayment systems. In the absence of intelligence information or evidence obtained from non-Cyberpayment system sources (e.g., physical surveillance) that trigger an investigation into specific suspect stored value instrument activity, peer-to-peer transfers of value are unlikely to be detected.¹

Transaction Anonymity. In some emerging Cyberpayment products, the origin of funds is relatively opaque and the identity of the individual or entity transferring them difficult to determine. In fact, payer anonymity (the identity of the party initiating a Cyberpayment value transfer) is a central characteristic of some proposed systems. For Cyberpayment value transfers (e.g., via the Internet or the telephone system), transaction anonymity could be an almost insuperable barrier to detection of illegal or suspicious activity by law enforcement. While candidate solutions for this problem have been put forward, they raise issues concerning individual privacy.

Denomination Limits and Value Characteristics. Cyberpayment product issuers are likely to limit the maximum amounts that can be stored on smart cards or other devices, to reduce the risks of fraud or other losses. As with credit cards, Cyberpayment issuers will also likely establish needs-based denomination limits that would be determined by commercial and market factors. (Recent consumer tests of Cyberpayment systems indicate likely consumer limits of approximately $1,000 to $3,000). Cyberpayment products held by retailers are likely to have a much larger value limit than those for most individuals and differ widely among retailers.

Cyberpayment value could also be programmed to expire after a certain number of transfers. As early technology adopters, money launderers could be expected to exploit whatever limits are established, just as they do now by structuring transactions under currency reporting limits, obtaining multiple cards (credit or debit), using multiple names, or employing multiple issuers.

¹ For information on recent developments in smart cards, see Mondex International’s web site, www.mondex.com. It should be noted that Internet-based e-cash systems, such as DigiCash’s e-cash product, allow for peer-to-peer value transfers without the use of smart cards. See www.digicash.com for details on the e-cash product.
The spread of these technologies may challenge established strategies for combating money laundering and financial crime. Criminals could seek to exploit the partial anonymity of Internet funds transfers to steal funds from unsuspecting consumers. In turn, encryption used in Internet transmissions of value could impede law enforcement's tracing of funds flows associated with suspected illegal activities. As the example in Figure 3.5 illustrates, Cyberpayments may also be used to revolutionize the process of money laundering, dramatically reducing the information available to law enforcement for investigations of potential wrongdoing.

![Diagram of Cyberpayments Abuse]

Figure 3.5 – A Hypothetical Example of Potential Cyberpayments Abuse

Lastly, differences in the oversight of Cyberpayment issuers in different jurisdictions may create opportunities to hide the true nature of lending or funds transfer activities - perhaps enabling individuals to launder funds without detection by law enforcement. Above is an example of Cyberpayment instrument abuse in which smart cards and the Internet enable the cover transfer of funds to an overseas location. The central feature of this type of transaction is the diminished availability of clear evidence that something illegal is occurring. This characteristic of Cyberspace is, of course, mitigated by the development of computer-based means for conducting surveillance of network traffic. It is generally believed, however, that sufficient means for identity concealment will remain in place, making it difficult to trace the activities of criminals in cyberspace. The design of new tools and techniques for this purpose may be a critical requirement in the future.

For additional information on the continuing rapid development of Cyberpayments instruments, consumer electronic funds transfer systems, electronic commerce, and illustrative commercial sites, see the following World Wide Web and print sources:


A Compendium of Information on Electronic Payment Systems
http://ganges.cs.tcd.ie/mepierce/project/oninternet.html

Mondex International – smart card-based Electronic Payment Solutions
http://www.mondex.com

Visa Cash – a reloadable stored value smart card product
http://www.visa.com/cgi-bin/vee/pd/cash/main.html??+0

American Express/Proton – A consortium offering reloadable and disposable smart card stored value products
http://www.protonworld.com

Cybercash - an Internet-based payment product
http://www.cybercash.com

Digicash – designers of an e-cash product
http://www.digicash.com
4. INTERNET BANKING

OVERVIEW

Internet banking is a new type of financial service created by the intersection of traditional retail financial services delivery and the emergence of the Internet. Internet banking involves the provision - over information networks - of basic banking services. These services include:

- Checking and savings accounts
- Certificates of deposit and other interest bearing instruments
- Consumer loans and mortgage financing
- Credit and debit cards
- Private banking services
- Currency exchange

It is important at the outset to differentiate between so-called “PC Banking” and true “Internet” banking. PC Banking allows owners of personal computers to access account information using a modem connection to a traditional bank or financial service provider’s corporate computer network. This access allows consumers to transfer funds within an established bank, to pay bills, and to transact other traditional financial services without entering a traditional branch office. Internet banking is similar to PC banking in that it allows the delivery of traditional financial services to customers through a home PC. What differentiates Internet banking from PC banking is the nature of the financial institution delivering the services to customers, and the importance of the public Internet to the provision of these products to the customers. Traditional banks have historically used private networks to deliver services to customers through personal computers or via the telephone (though this is changing). Internet banks may not possess a physical branch network at all. Instead, these entities may operate secure network servers in a variety of locations, with only a small number of human personnel to handle customer queries. Internet banks may deliver financial services to customers from almost any location, and to almost any location, thus posing potentially onerous tasks for regulatory authorities.

ENABLING TECHNOLOGIES

The Internet is enabling the replacement of retail banking outlets by individual consumer interaction with financial services through personal computer software. The near ubiquity of Internet connectivity enhances the ability of consumers to initiate funds transfers, pay bills, and gain access to account information without setting foot in a branch location. The deployment of such security technologies as the Secure Socket Layer (SSL) and Secure Encryption Technology (SET) protocols means that consumers will be able to transact banking business in relative safety, protected from the theft of their account numbers or credit/debit card information by hackers and other criminals.¹

The expansion in Internet connectivity is the focal point for this nascent industry. The wide availability of Internet access through local, national, and international Internet Service

¹ For information on the SET protocol, see http://www.setco.org/.
Providers (ISPs) provides the critical infrastructure for consumer data communications with participating banks. In turn, software products have evolved to make the interface between consumers and financial services offered by banks as user friendly as possible. Taken together, these trends point toward the accelerating expansion in the Internet delivery of financial services, and to a significant change in the structure of the financial services industry.²

THE ECONOMICS OF DEPLOYMENT

Internet banking allows financial service providers (banks and their competitors) to minimize transactions costs in their business operations. Transactions costs - the costs of delivering products (e.g., checking and savings account services, credit and debit cards) to their customers - are a significant drag on profit margins in business and reduce the overall efficiency of an enterprise. Costs fitting into this category include the expense of buildings, personnel, and whatever physical infrastructure is necessary for the delivery of retail banking services through a network of branches. Because Internet banking notionally requires a lower personnel level for the delivery of basic financial services, it offers a potentially dramatic reduction in bank operating costs and a parallel potential increase in profitability.³

For consumers, the added convenience of banking through their personal computers also means that they may face lower charges for banking services (though this is far from certain). Some banks are introducing new charges for services delivered through branches, thereby enhancing the relative attractiveness of their Internet-delivered products. It is likely that such tactics will continue, driving consumers toward a much more Internet-based financial services delivery standard.

Operating Entities in Internet Banking

A number of different entities are likely to offer Internet banking services. Traditional financial service providers will of course be present. These include

- Banks
- Credit Unions
- Stock Brokerages
- Money Services Businesses (MSBs).

The more competitive environment of the financial services industry will also likely include new entrants, empowered by the lowered costs of service delivery over the Internet. Examples of these new actors include

- Telecommunications Companies
- Computing Companies
- Internet Service Providers.

² It is possible that this changed economic environment is also part of the current financial industry restructuring process.
³ See Department of Commerce, The Emerging Digital Economy, pp. 24-35.
THE SPECIAL CASE OF OFFSHORE INTERNET BANKING

Offshore banking centers are “offshore” to the extent that they deliver financial and corporate services to non-residents of the banking center’s jurisdiction. As a document by the Offshore Group of Banking Supervisors argues:

The term “Offshore” is interpreted by some as meaning that the location in which services are provided is itself “Offshore”; for example, an island in the Caribbean or the Pacific. In fact the term should be used to describe the actions of the citizens of individual countries who wish to enjoy financial services outside their own jurisdiction in centres that offer certain freedoms otherwise not available to them.\(^4\)

From this perspective, the “Offshore” activity relates to the behavior of the customer, not that of the institution delivering the financial or business services. In short, “offshore” can refer to financial services being offered to a customer whose home jurisdiction is unable or unwilling to provide them.

In this sense, offshore Internet banks are “offshore” not only because their Internet servers may deliver banking and financial services across an international border without the necessity of physical travel by the customer seeking available products, but also because their servers can be located in jurisdictions with more stringent confidentiality provisions than their “onshore” counterparts. In a sense, the customer’s PC becomes equivalent to a branch office of a foreign financial service provider. Increased confidentiality, coupled with problems of determining the jurisdiction of Internet transactions, and the difficulty of tracking such transactions, combine to make Internet offshore banks a serious new challenge to established oversight mechanisms.

Currently available banking services in the Internet “offshore” domain include

- Incorporation
- Currency Exchange
- Trading of Stocks and Bonds, Portfolio Management
- Letters of Credit, Loans
- Numbered Accounts
- Insurance Products
- Establishment and maintenance of trust agreements.

Law enforcement and regulatory authorities throughout the world share a concern that criminals may seek to use offshore financial centers operating on the Internet to launder money and commit financial fraud. In particular, criminals may seek to (1) exploit weaknesses in Internet bank internal controls and government oversight to conceal money laundering and financial fraud; (2) utilize “secrecy havens” to impede international investigations of suspected criminal activity by exploiting differences in encryption laws and bank secrecy to conceal potential evidence; or (3) operate a wholly fraudulent Internet bank to defraud customers.\(^5\) The following figure provides a schematic of one method of concealing funds transfers generated at an offshore Internet bank from law enforcement authorities in one’s home country:

\(^5\) For a description of an Internet bank eventually used to defraud customers, see http://www.isaco.co.uk/cminewes/library/content/itn/newswire/page6d72.htm.
A customer opens an account in an Internet bank headquartered in a foreign jurisdiction.

A customer then orders a payment from that account to purchase goods or services in a third jurisdiction.

Finally, goods are delivered in payment of a debt in a fourth jurisdiction.

Figure 4.1. An Example of Concealed Funds Transfers using Cyberpayments and an Internet Bank

A few features stand out in this example. First, the only place where the home government can be assured of gaining information on the nature and type of financial activities initiated from the personal computer is if it has some sort of investigative device or third-party knowledge giving it information on the financial activities being generated from where the PC is located. Second, once the customer initiates funds flows from a foreign Internet bank, regulators in the first jurisdiction are wholly dependent on relationships (and laws) in the jurisdiction where the Internet bank resides for information regarding the identity of account holders. This means that Internet bank jurisdictions may exercise a critical “withholding” function that may impede investigations of fraud or money laundering, which require revealing the secret identities of “numbered” account holders.

These and other challenges confront a fragmented international regulatory regime that seeks to come to grips with a new environment - offering an ability to reach beyond borders to both deliver and receive financial services.

For more information on Internet banking and the technologies online financial services please consult the following web sites:

Security First Network Bank
http://www.sfnb.com/

Online Banking and Financial Services Directory
http://www.orcc.com/banking.htm
Citibank
http://www.citibank.com

Atlanta Internet Bank
http://www.atlantabank.com

Caribbean Banking
http://www.caribinfo.com/directory/cbuslinks/cbank.htm

Cybank Corporation – Internet Banking and Bill Payment
http://www.cybank.com

Banknet Internet Banking
http://mkn.co.uk/banknet/
5. INTERNET GAMBLING

OVERVIEW

In 1997, the total volume of wagering from the legitimate casino gambling industry in the United States was $535 billion. Before Internet-based gambling opportunities can claim a significant share of this market, a number of issues must be addressed, not least of which are decisions regarding the regulatory oversight of gambling operators.

Internet gambling has many characteristics in common with other services designed for delivery over the Internet. Internet gambling is a relatively new phenomenon but can be defined roughly as the provision of opportunities to play games of chance or obtain access to sports or race bookmaking via computer networks. It is also possible that Internet gambling products could be delivered using proprietary software; however, emerging applications appear to be adopting the World Wide Web as the preferred interface.

As in other areas of electronic commerce, privacy and security are primary concerns for both users and service providers. The fact that gambling is illegal in some localities - and subject to social disapproval in others - means that the Internet may foster an increase in such activities due to the use of personal computers and the expanded possibility of anonymity.

MODES OF INTERNET GAMBLING

Cyberpayment instruments and Internet banking may provide the funds for initiating gambling activity on the Internet. An example of Cyberpayment value used in gambling is an instance where a consumer transfers value from his or her home computer to an online casino for the purposes of gambling. In this case the funds transferred constitute the player’s stake. The transfer utilizes the peer-to-peer capabilities of the Cyberpayment instrument or the electronic funds transfer capabilities enabled by the availability of an Internet bank. Remittances of winnings are transferred to players through the same facility, either through direct transfers to a Cyberpayment instrument (e.g., a stored value smart card), or transfers to an account maintained at an Internet bank. The potential rapidity of such transactions makes third-party monitoring of gambling activity on the Internet a potentially significant challenge. At the same time, however, if Internet gambling system operators are subject to close regulation, post hoc inspection of transaction records might make a partial reconstruction of gambling patterns possible.

Another type of Internet gambling is an electronic version of sports bookmaking, where players bet on the outcomes of such sporting events as baseball, basketball, football games, or horse racing. Analogous to gambling activity already taking place in Las Vegas and elsewhere, this type of activity would again involve the transfer of electronic value from players to a gambling establishment (and vice versa) through the Internet. Player confidence in the credibility and honesty of the gambling operator is obviously central to the viability of Internet bookmaking, but the potential gains - in terms of large winnings and relative secrecy - may convince some gamblers that heightened risks are worth taking.

While the first generation of Internet games are likely to be simple electronic versions of conventional casino gambling situations, novel gambling applications are likely to emerge. This
pattern, first-generation applications based on “real world” models and second generation applications representing entirely new “Internet-native” products, has already been observed on the World Wide Web and in other electronic commerce situations.

Funds Transfer Vehicles for Internet Gambling

In addition to the use of conventional paper checks and cash, new electronic payment instruments may be used to transfer funds to Internet casinos or other network-based gambling establishments. In this case, two types of electronic payment facilities are central: Cyberpayment Systems (providing digital cash or e-cash), and Internet banking. Both of these electronic funds transfer environments allow for varying levels of anonymity in the placement of stakes. While the features of Cyberpayment instruments vary (see Chapter 3 for an illustrative overview of these payment instruments), they all provide increased rapidity of transactions, an enhanced ability to engage in transactions at geographic distance, and reduced exposure to regulatory and law enforcement authorities.

In this direction, the immediacy of the Internet gambling experience is restricted by some of the same technical shortcomings that also inhibit the emergence of other electronic commerce applications. Bandwidth restrictions which limit data transmission, and consumer apprehension regarding security are two significant barriers to widespread acceptance of Internet gambling. Both concerns are likely to be resolved by technological advances, most importantly in the areas of new Internet technologies that yield faster connections and stronger encryption techniques for the protection of consumer financial information. The marketplace has yet to reveal what critical mass of applications and opportunities will make the industry take off. If the emergence of the World Wide Web is any guide, Internet gambling will likely take its place alongside other network-based economic activities once technical standards - and the physical network links of the GII - are in place.

Internet gambling has much in common with other forms of electronic commerce. If Internet gambling is to persist it will most likely have to meet at least four criteria for service delivery which also have importance for other forms of electronic commerce: (1) immediacy, (2) security, (3) cost-efficiency, and (4) anonymity. These issues are expanded on below.¹

Immediacy - Payout of winnings must immediately follow a game, or users may suspect fraud on the part of gaming operators.

Security - Information regarding gambling may be sensitive and must remain closely held. Also, funds transfers must remain protected from inadvertent theft or inappropriate charges. The integrity of gaming establishments themselves supports this issue, as consumer concerns with fraud must be minimized if Internet gaming is to compete with traditional gaming and entertainment products.

Cost Efficiency - Minimizing transaction costs is central to providing players with enhanced winning opportunities and gambling operators with more favorable operating margins.

Anonymity - Gamblers on the Internet may wish to preserve their privacy - both from government authorities and the gambling operator. The security of transferred funds and of credit or debit card numbers must be maintained to prevent the identification of players by unauthorized third parties.

¹ For an in-depth analysis of the evolution of Internet Gambling, see Anthony Cabot (ed.), Internet Gambling Report II (Las Vegas: Trace Publications, 1997).
These criteria intersect directly with the central features of Internet-based payment products. Cyberpayment instruments and Internet banking opportunities allow consumers to enjoy the immediacy of Internet gaming while enjoying access to funds in a safe and sound financial service environment. Internet-based payment solutions meet the following four important considerations regarding gambling on the Internet:

- They provide an adequate system for funds transfer.
- They provide means for securing gambling transactions from hackers.
- Utilization of funds deriving from the legitimate financial services environment may assist in mitigating questions regarding the integrity of an Internet gambling operator.
- Legal issues governing Internet gambling may be partially mitigated because of the settled legal environment (in relative terms) governing established financial institutions.

It would be a mistake to idealize Internet-based gambling opportunities as a somehow “inevitable” next step in the evolution of the gambling industry. As is true in other areas of electronic commerce, consumer acceptance of the type and frequency of gaming opportunities is the critical step in establishing the financial viability of a gambling enterprise.

Internet gambling operators will likely compete against traditional gambling establishments for patrons. If Internet gambling is legal in their jurisdictions, traditional casinos and gambling establishments are also likely to offer Internet gambling opportunities - if only to protect their established businesses. This makes likely some sort of “shake-out” among Internet gambling providers similar to what is currently taking place among ISPs. In the broader ISP arena smaller firms are either being acquired by larger firms or are going out of business, unable to compete on price with larger operators. In Internet gambling as well, the established reputations for running an honest game may prove to be the most valuable means for sustaining a viable business on the Internet. Because gambling is subject to such varied regulation around the world, safety and security - often seen as synonymous with an established brand name - may prove a valuable means for the industry to establish itself as a legitimate enterprise.

In addition, Internet gambling operators will have to face the realization that virtually any type of gambling activity is vulnerable to money launderers and other types of financial criminals. In July 1998, FinCEN published a report entitled “Suspicious Activity Reporting & Casinos” which discusses, among other topics, the process of money laundering, the vulnerability of casino gambling to money laundering, and the methods for detecting and reporting suspicious activity which can occur through casinos in the United States. Also, this document provides an illustrative list of suspicious examples. The underlying activities for some of these examples may also occur in an Internet gambling environment.

Internet gambling may change the ways in which gamblers are able to pursue their fascination with games of chance. The challenge to oversight authorities remains to find ways to prevent illicit activities while allowing legitimate gambling operators and players to conduct their business in an open and potentially lucrative setting safeguarded by a sound and comprehensive regulatory regime.

For additional information on Internet gambling please examine the web sites listed below:

---

2 In July of 1998, the U.S. Congress sought to ban Internet gambling entirely. The availability of Internet gambling from sites based in the Caribbean places in question the U.S. government's ability to enforce such a ban.
Caribbean Casino
http://www.casin.org

Centrebet
http://www.centrebet.com.au

Worldwide Tele Sports
http://www.wwrs.com/

Casinos of the South Pacific
http://www.cosp.com/

English Harbour Casino
http://www.englishharbour.com/

Atlantis Gaming
http://www.atlantis-gaming.com/

Caribbean Cyber Casino
http://www.ccasino.com/

Casino Royale
http://www.funscape.com/

Omni Casino
http://www.omni.casinocom/index.htm
6. EMERGING DIMENSIONS OF THE CRIMINAL EXPLOITATION OF ELECTRONIC COMMERCE: POTENTIAL PROBLEMS AND SOLUTIONS

INTRODUCTION

The potential for the criminal exploitation of cyberspace-based payment systems flows from the basic nature of the products and services made possible by the information revolution. Technologies providing relative consumer anonymity and increasingly rapid disintermediated funds transfer will likely enable new forms of money laundering and financial fraud. In this way cyberspace is no different from any other environment in which human beings interact with one another. The balance between law enforcement detection techniques and the complexity of criminal activity will likely be different in the information age, however. A number of key questions arise from this observation: First, how serious will the problems of criminal activities in cyberspace become? And what law enforcement and regulatory responses exist to mitigate perceived problems?

This chapter presents examples of cybercrime deriving from contemporary experience with money laundering and financial fraud. It begins with a basic description of money laundering and then gives hypothetical examples of these activities in the physical and cyber environments. The second part of this chapter provides a summary of potential technologies that may offer law enforcement and regulatory authorities capabilities for combating illegal activities in cyberspace.

DEFINING MONEY LAUNDERING

Money laundering is a process through which criminal proceeds take on the outward appearance of legitimacy. It is an integral support function common to virtually all profit-producing criminal activities and in many countries is itself an illegal activity. Criminals or criminal organizations engage in money laundering to conceal the origin of funds, repatriate profits, and remove money from possible seizure by law enforcement officials. The process of laundering money traditionally entails three stages – placement, layering, and integration.

Placement

Placement is the first stage in the money laundering process and is where illegal proceeds are most vulnerable to detection. It is during the placement stage that currency enters the financial system. When illicit monies are deposited at a financial institution, placement has occurred. The purchase of money orders using cash from a criminal enterprise is another example of placement.

Layering

Layering describes an activity intended to obscure the trail that is left by dirty money. During the layering stage, a launderer may conduct a series of financial transactions in order to build layers between the funds and their illicit source. For example, a series of bank-to-bank wire transfers, would constitute layering. Activities of this nature, particularly when they involve funds transfers between tax haven and bank secrecy jurisdictions, can make it very difficult for investigators to follow the trail of money.
Integration

During the final stage in the laundering process, illicit funds are integrated with monies from legitimate commercial activities as they enter the mainstream economy. The illicit funds thus take on the appearance of legitimacy. The integration of illicit monies into a legitimate economy is very difficult to detect unless an audit trail had been established during the placement or layering stages.

MONEY LAUNDERING SCHEMES

Money laundering schemes may vary greatly in character and complexity. They may involve any number of intermediaries; utilize both traditional and non-traditional payment systems; and be domestic or international in nature. To a large extent, the scope and nature of a money laundering operation is limited only by the creativity of those involved.

For example, international narcotics traffickers may employ a variety of money laundering techniques and schemes at any one time. Each money laundering scheme may be specially created to fulfill very specific goals and objectives. Advanced computing and communications technologies are routinely used to enhance the efficiency and the security of today's narcotics-related money laundering operations. The examples that follow below are baseline schemes intended to familiarize the reader with a few simple methods for moving illicit funds.

Example 1 (Figure 6.1)

Objective: Move U.S.-based funds to Mexico for use in local economy.

1. Street level narcotics sales occur in the U.S. Cash is the preferred method of payment for these transactions.

2. The cash from one or multiple sales locations is collected at a safe or "stash-house" for processing.

3. The cash is taken to a remittance business for transmission out of the U.S. To avoid scrutiny by law enforcement or bank regulatory authorities, the cash may be divided into amounts less than $10,000 and "smurfed" or structured at the remittance business.

4. The U.S.-based remitter deposits funds in U.S. bank.

5. The U.S. bank transfers funds to Mexico.

6. The Mexican bank pays the remitter in Mexico.

7. Remitter in Mexico pays out in Pesos.
Figure 6.1 - Movement of Funds from the U.S to Mexico

Examples of hypothetical money laundering schemes involving Internet or Cyberpayment funds transfers are not difficult to construct. Two examples follow. In each case, the rapidity and relative anonymity of Cyberpayment funds transfers offer potential avenues for criminals to avoid detection by law enforcement authorities.

Example 2 (Figure 6.2)

Objective: Move U.S. based funds to offshore bank for future repatriation to U.S.

1. Street level narcotics sales occur in U.S. "Disposable" stored value cards are used for individual transactions.

2. Funds are collected at merchant terminal and transferred on to a single high-denomination stored value card for further movement.

3. Funds are transferred from high-denomination stored value card over a cellular telephone to an offshore bank.
Example 3 (Figure 6.3)

Objective: Launder U.S.- based funds for use by cartel associate in Antigua.

1. Street drug deals are executed using disposable stored value-type smart cards.

2. Smart card value is uploaded onto a PC.

3. Value is sent as an attachment to an e-mail message through an anonymous remailer located in Finland.

4. Value is received by a drug cartel associate at his PC in Antigua.
AN OVERVIEW OF POTENTIAL LAW ENFORCEMENT RESPONSES

A number of information technologies have potential applicability to law enforcement investigations and regulatory oversight of cyberspace-based payment systems. The convergence of computer, network, and telecommunications technologies is creating an infrastructure for the crossborder delivery of products and services for consumers and businesses. This same infrastructure requires a system of authentication for the identities of persons and entities operating in cyberspace and a secure system of accounting for the exchange of funds. These requirements create a nascent record-keeping structure that may be of use to governments in conducting legitimate regulatory and law enforcement activities.

Because a variety of systems of authentication and security for electronic commerce are being put in place by the private sector, governmental concerns with data gathering and the analysis of information obtained from networks may receive secondary treatment. It is not sufficient to assume that existing law enforcement and regulatory data gathering and analysis requirements will be met by the private sector. Instead, the deliberate application of data manipulation technologies is critical to maintaining the investigative capabilities of government authorities. Investments by government in data analysis tools may be critical to ensure the creation of such specialized capabilities. To this end, a number of the technologies being

---

1 The exact size and scope of appropriate government investments in this area is itself controversial. Traditionally encryption and computer-based information gathering has been the realm of national security or intelligence agencies. As the information age emerges, however, new lines are being drawn as law enforcement authorities seek to preserve established information access, and perhaps, to secure such new access as technology allows. For an exploration of some of these issues in the US context, see Bruce
deployed by the private sector in electronic commerce may offer new ways of providing information to appropriate government authorities. This chapter outlines some of these systems, and discusses their potential contributions to combating financial crime in cyberspace.

The Technologies in Question

Technologies that may contribute to the gathering of information on data flows and the identities of those operating on the Internet can be grouped into three categories, (1) record keeping systems, (2) authentication measures, and (3) tracking systems.

**Record Keeping Systems.** Electronic record keeping of e-commerce transactions presents a potentially lucrative data source for law enforcement and governmental regulators. These systems typically collect information on the nature of network traffic, allowing network managers to characterize broad trends in user access. Record keeping systems collect information through the creation of a set of server logs that record the time of an online transaction, the duration of an online session, and identifying information relating to the network address of the consumer or business initiating the transaction. Network logs of this type can form the basis of more sophisticated analysis of network traffic. Basic data can be subjected to more sophisticated analyses through the use of “profiling techniques,” whereby artificial intelligence techniques are used to detect patterns of transaction activities associated with suspected money laundering or cyberspace financial crime.

Analysis of network traffic is one quick means of gaining a broad appreciation of the structure and timing of electronic commerce. It allows e-commerce companies to “narrowcast” their products to particular customers according to their likely interest in purchasing items, and creates new information when databases of customer transactions are compared to information from credit reports and online directories. “Data mining” of consumer transactional data is a set of techniques used to find associations between consumer transactional behavior and credit worthiness and other demographic data of interest to marketers. Data mining is performed by statistical software packages installed on high-powered computer work stations. Such analytical tools may also be of use to law enforcement authorities and regulators to discern patterns in transactional data associated with criminal activity.²

**Authentication Measures.** Authentication measures allow network operators and government authorities to identify individuals or entities involved in online commerce. Two technologies are representative of this capability:

**Digital Signatures** - a label attached to e-mail, data, or electronic value flowing within a network that authenticates the identities of particular individuals or entities. Tied to particular transactions, digital signatures create an electronic trail, linking online transactions with particular individuals.

**Biometric Forms of Identification** - hardware and software systems that authenticate the identities of human beings through the capture of unique data characterizing a person’s physical features.

² The mathematical challenge of tracing network traffic on the Internet should not be underestimated. It is believed, however, that continuing progress in network and computing speed may make this problem more tractable in the future.

Examples include images of a person’s fingerprint or palm print, a laser-scan of an individual’s retina or iris, and a voiceprint.

Electronic traces of online activity raise concerns regarding consumer privacy and potentially inappropriate uses of sensitive information by unauthorized persons. It is important then to consider these techniques in relation to the regulatory and law enforcement purposes that they may support. It is nonetheless true that the electronic infrastructure to perform many of these activities will likely emerge as a consequence of the growth of electronic commerce.

Entities providing funds, goods, and services over the net are necessarily concerned with ensuring the safety and security of their transaction systems from compromise by hackers or thieves. Additionally, network providers of financial services must meet established regulatory concerns relating to their abilities to identify customers. These concerns mean that some type of authentication and record-keeping system is necessary for a vibrant electronic commerce arena.

**Tracking Systems.** Network tracking systems are, perhaps, the most experimental of all of the techniques becoming available for conducting surveillance over online activities. Still in research are techniques deriving from already deployed artificial intelligence (AI) applications that use knowledge-based systems to characterize network traffic according to such criteria as point of origin, duration of online session, and identity of the user. The major difference with these techniques is that they are implemented in software analogous to that of a computer virus.

Network-borne tracking systems are of two broad types: (1) classifier systems, using rule-based models derived from the judgement of human experts; and (2) software agents with elementary machine “learning” capabilities that are reinforced by continual exposure to transaction data in a network setting.

The combination of record keeping systems, authentication measures, and tracking systems yields an infrastructure of potential use to law enforcement and government regulators in establishing the money - illicit activity nexus so important to the building of a case for potential prosecution.

Each of these tools has the potential to conduct partially or completely autonomous data-gathering activities – in some sense analogous to motion or temperature sensors in the physical world. Development of these tools is at the speculative “outer-edge” of research, and their true potential for intercepting potentially suspicious electronic commerce activity remains to be demonstrated.³

**CHALLENGE AND RESPONSE IN RETROSPECT**

Each of the tools and techniques listed here is likely to appear in the near future. It is important, however, to remain focused on the most significant barriers to near- and medium-term law enforcement and regulatory responses to cyberspace crime. Even if the technologies are available, it is clear that an appropriate legal framework must be created within which these technologies may be applied. Because legal and policy changes typically occur at a much slower rate than does technological change, a level of uncertainty exists regarding the arrival of

appropriately modified (or new) legal regimes designed to cope with the special realities of the cyberspace environment. Coming to grips with this potential discontinuity in legal and technological environments is one of the tasks undertaken by participants in Step Three of the exercise. The next chapter outlines some of the legal and regulatory challenges significant to this effort.
7. REGULATORY, LAW ENFORCEMENT, AND LEGAL ISSUES

INTRODUCTION: E-COMMERCE AND GOVERNMENT OVERSIGHT

Cyberpayment instruments, Internet banking, and Internet gambling - the focus of the exercise - represent three principal emerging elements of electronic commerce (e-commerce). Traditional regulatory and law enforcement methods for countering financial crime may be challenged by such e-commerce developments.

During the course of the exercise participants were asked to consider the potential efficacy and importance of taking action in four general categories in two distinct regulatory dimensions – (due diligence and oversight and supervision) - and in the law enforcement and legal realms:

1. **Due Diligence.** Measures taken by financial services providers under regulatory supervision to ensure the integrity of those conducting business with the institution.

2. **Oversight and Supervision.** Regulatory policy and enforcement responsibilities of government authorities with regard to financial service providers.

3. **Law Enforcement.** Issues regarding the application and effectiveness of traditional investigative programs, tools, and techniques.

4. **Legal.** Issues regarding the application and effectiveness of existing legal structures (i.e., the statutory base from which to investigate cyberspace-based crime) as they pertain the inherent cross-jurisdiction nature of Internet-based financial transactions.

A more detailed description of each of these four issue categories is given below.

DUE DILIGENCE

Under the Due Diligence heading, four sub-categories of regulatory issues can be identified:

- Identification
- Know Your Customer
- Record Keeping
- Suspicious Activity Reporting

Identification

When establishing customer relationships, financial service providers take steps to ensure that transactions are conducted by the lawful individuals known to the institution. In the cyberspace environment, however, authenticating a transactor's identity may present new challenges to the financial institution.
New electronic and biometric techniques are being developed that may allow financial service providers to accurately identify customers in the cyberspace environment. Many of these techniques employ advanced computational and imaging technologies.

For example, accounts with access to stored value smart cards may require the filing of a digital signature with a trusted certification authority. This would ensure that financial institutions would have information regarding the initiator of funds flows through their servers - which could be obtained by law enforcement authorities on presentation of the required legal permissions. In turn, this digital signature may be related to the provision of biometric identification information again filed with a trusted certification authority whose records may be subject to subpoena by law enforcement agencies.

Examples of biometric systems include retinal scanning, voice print identification, and fingerprint imaging. Issuance and use of certain Internet banking products and services might, for example, require the use of biometric identification techniques at the computer terminal or smart card reading device where the transaction is to be initiated.

**Identification issues discussed during the exercise included:**

- Employing biometric techniques and identification requirements for such applications.
- Employing digital signatures and encryption to establish a safe secure infrastructure for the authentication of digital transmissions.

**Know Your Customer**

Know your customer (KYC) concerns arise from the potentially anonymous characteristic of Internet-based financial transactions or, when communicating with a purported account holder about such transactions. If a financial service provider is only in contact with a customer through electronic means, how is it to authenticate the identity of a person while conducting financial transactions.

It is possible that Cyberpayment system operators, Internet banks, and Internet gambling establishments will be required to meet special KYC information requirements in order for them to obtain licenses to deliver certain classes of financial products over the Internet. This may include the electronic filing of special identification documents by any account holders with access to a defined class of electronic payment products.

**KYC discussed during the exercise included:**

- Defining unique identity authentication requirements for certain classes of cyberspace financial products and services.
- Developing international norms for cyberspace “Know Your Customer” measures and procedures.
- Developing monitoring and enforcement infrastructures for coordinating cyberspace “Know Your Customer” rules and regulations.
Record Keeping

In almost all nations standards exist for the filing and maintenance of records pertaining to all financial transactions conducted through regulated institutions. In the realm of electronic commerce, however, some types of transactions may fall outside the scope of existing record keeping regulations.

Good records of e-commerce transactions would greatly assist investigators searching for potential cyberspace crime. If such records were generated automatically by merchant electronic commerce transaction systems, law enforcement would gain a potentially valuable tool for combating financial crime on the Internet.

The dissemination of information gained from electronic transaction records would itself be subject to legal and administrative guidelines. Two basic questions flow from this realization:

1. Should such records be shared internationally between investigating jurisdictions?
2. Should aggregate data be shared, or more “fine grained information” on the identities of individuals who are the subject of ongoing criminal investigations?

Decisions on these issues could be made on a case-by-case basis or through a generalized rule - perhaps embedded in a bilateral or multilateral memorandum of understanding. It is clear that the differences in rules regarding information sharing have considerable importance for coordination of oversight and law enforcement investigations relating to cyberspace crime.

Record keeping issues discussed during the exercise included:

Coordinating record keeping requirements in electronic commerce applications.

Sharing of information in cyberspace financial crime investigations.

Providing incentives for good behavior by Internet banking, Internet gambling, and Cyberpayment financial services providers.

Monitoring of network data in real time to detect cyberspace financial crime.

Suspicious Activity Reporting

Suspicious Activity Reporting (SAR) has been recognized in many international fora as an effective anti-money laundering tool. SAR programs of varied character have been developed, each taking into account regional and industry differences and practices. The same flexibility will be necessary when establishing SAR criteria for cyberspace. Are activities that are considered “suspicious” and therefore reportable in the brick-and-mortar banking world, the same activities that should cause concern if observed in the Internet banking context?

Electronic forms of suspicious activity reporting could be mandated for Cyberpayment system, Internet Bank, and Internet gambling institutions. These systems could be based on a
technique known as “profiling,” whereby artificial intelligence techniques could be used to study network traffic at a regulated institution’s servers as a means of differentiating criminal activity from “normal” business activities.

Computer-generated suspicious activity reports would also be of potential utility if they were shared with other countries. A dedicated secure information system designed to facilitate this kind of information sharing might help agencies coordinate their investigative activities.

| Suspicious Activity Reporting issues discussed during the exercise included: |
| Reporting electronic suspicious activity reporting and cyberspace financial crime. |
| Sharing of electronic suspicious activity reports. |
| Establishing cross-jurisdiction rules for electronic information sharing. |

OVERSIGHT AND SUPERVISION

Oversight and Supervision refers to the regulatory policy and enforcement responsibilities of governmental authorities with regard to financial service providers.

The oversight and supervision category can be divided into three components:

• Licensing
• Payment Instrument Functionality
• Examination

In terms of licensing, although most nations have established regulations pertaining to banks and other financial service providers, potentially unique licensing requirements may be associated with institutions that operate in cyberspace.

| Licensing issues discussed during the exercise included: |
| Establishing rules governing permissible operators of Internet gambling establishments, Cyberpayment systems and Internet banks. |
Payment System Functionality issues discussed during the exercise included:

Collaborative information gathering at Internet banks

Techniques for “on-site” inspection in cyberspace

Remote surveillance of Internet financial services providers

Also within the scope of the oversight and supervision, comes the issue of payment instrument functionality. As electronic commerce emerges, some nations have taken regulatory and legislative measures to mandate the operating characteristics of Cyberpayment, Internet banking, and Internet gambling products. However, other nations have chosen to “wait and see” how the industry develops. See the above box for the treatment of these issues articulated within the exercise.

Examination also plays a key role in the oversight and supervision process and presents potentially significant challenges in the cyberspace context. The rules and techniques for auditing financial activity on the Internet are still being developed. The issue of examination becomes more complicated when raised in the context of activities that may occur in or have an effect on multiple jurisdictions.¹

Examination issues discussed during the exercise included:

Role of mandatory filings in international oversight activities

Extra-territorial investigations of offshore Internet banks

Extra-territorial investigations of offshore Internet gambling establishments

Oversight and jurisdiction questions concerning international cyberspace financial services operations.

LAW ENFORCEMENT ISSUES

Governmental authorities have developed progressively more effective mechanisms and techniques for the investigation of money laundering and other financial crime. However, these investigative techniques were created within the context and limitations of the traditional payment system. With the advent of electronic commerce, these proven law enforcement programs must be continually assessed to determine their effectiveness.

¹ In the future, networking technology could route individual transactions to any one of many available servers around the world, dynamically routing them in real time. Jurisdictional issues in this setting would be even more complex than on the contemporary Internet. We would like to thank Robert Anderson for providing this insight.
Law enforcement issues discussed during the exercise included:

- Determining the relevance of wiretaps and other means of electronic surveillance.
- Employing tools and techniques for intercepting communications over computer networks.
- Determining the utility of undercover operations in investigating cyberspace financial crime.
- Determining the role of confidential informants in investigating cyberspace financial crime.
- Determining the role of mandatory filings in combating cyberspace financial crime.
- Meeting privacy concerns in obtaining law enforcement access to cyberspace financial records.

Within this context, technology may present both challenges and opportunities for law enforcement. The Cyberpayments, Internet banking, and Internet gambling components of electronic commerce, if left unchecked could be vulnerable to exploitation for criminal purposes and may compel authorities to consider and/or develop new investigative techniques. At the same time, however, the new technologies, by virtue of their operating characteristics, may also facilitate innovative cyberspace-based investigative tools by providing new and automated means to collect relevant information.

Law enforcement concerns with the rise of Internet-based financial services focus on the availability of information that can serve as the basis of an investigation and - if warranted - subsequent prosecutions. For example, what is the basis for exploiting wiretaps and other means of intercepting communications over computer networks? All traditional law enforcement techniques must be evaluated in this context. See the above text box for the exercise treatment of these issues.

LEGAL ISSUES

There are various legal issues related to the emergence of cyberspace-based payment systems. Some countries may lack the statutory base from which to investigate and prosecute cyberspace-based crime. Others may lack the rules of evidence to utilize certain types of information unique to cyberspace. In addressing this concern, some nations attempt to apply or modify existing law to fit the cyberspace environment. In some instances, new laws are being enacted to focus specifically on cyberspace-based criminal activity.

Even more challenging international legal and jurisdictional problems may appear due to the “borderless” nature of cyberspace. Even if appropriate cyberlaws exist in a particular
country, could or should they apply in instances where some of the activity may have occurred in multiple jurisdictions? Complicated issues, such as timing, must be addressed in international fora to ensure some degree of compatibility among jurisdictions.

The status of “evidence” in the context of Internet gambling records, Internet banking records, and Cyberpayment transaction records deriving from a foreign legal jurisdiction will be a particularly difficult issue. Information sharing and complementary regulatory approaches that strengthen international oversight will likely require new collaborative arrangements between national law enforcement and regulatory authorities. Another set of problems concerns the activities of an Internet casino whose services are available in a locality where gambling is illegal.

In these contexts, criminals may seek to exploit differences in national law to avoid prosecution for illegal activities in cyberspace. Preventing this occurrence will require the coordinated actions of the international community and some agreement on a framework of rules for the rapidly expanding electronic commerce environment.

<table>
<thead>
<tr>
<th>The international legal issues discussed during the exercise included:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establishing comparable laws and regulations governing cyberspace financial crime.</td>
</tr>
<tr>
<td>Seeking common definitions of “legitimate” and “illegitimate” cyberspace financial activity.</td>
</tr>
<tr>
<td>Determining the admissibility of computer records in international cybercrime investigations.</td>
</tr>
<tr>
<td>Determining the role and utility of traditional legal mechanisms, such as Mutual Legal Assistance Treaties (MLATs) and Letters Rogatory, in combating cyberspace crime.</td>
</tr>
<tr>
<td>Exploring extraterritorial issues and the determination of appropriate jurisdictions in the investigation and prosecution of cyberspace crime.</td>
</tr>
</tbody>
</table>

Each of the elements listed above formed a part of the universe of issue area choices confronting exercise participants. The next chapter summarizes their discussions on these issues and reports on the choices that they made in the context of the exercise scenario.
8. EXERCISE FINDINGS

INTRODUCTION

Over the course of the exercise test series a universe of issues was used to define the broad landscape of governmental concerns raised by the emergence of cyberspace-based payment systems. The set of questions developed during the exercise was the result of a series of expert-level discussions involving government and industry participants conversant with legal and law enforcement issues specific to the Caribbean region. Much of the focus was on money laundering and financial fraud, but discussions among participants extended to a broader inquiry into the legal and economic consequences of the emergence of the information economy.

Discussions within the exercises were structured by group leaders charged with focusing participant activities around the core set of issues regarding international money laundering activity. The scope of discussion was further narrowed by the scenario-based examination of controversies targeting specific features of Cyberpayments, Internet banking, and Internet gambling. Participants in the exercise were confronted with a universe of issues subdivided into four major categories:

- Due Diligence
- Oversight and Supervision
- Law Enforcement
- Legal

Participants were asked to rank the issues and subsidiary questions in the above categories in order of significance. This rank ordering was obtained at the end of lengthy discussions on the impact of scenario features on law enforcement investigations, prosecutorial activities, and regulatory oversight. Participant rank orderings were then selected and tabulated to create an overall appreciation of the priorities for future action in combating potential abuses of electronic commerce.

While no clear consensus on how to address problems and dilemmas created by potential patterns of abuse in electronic commerce emerged, a high degree of agreement was visible in areas where government policymakers and law enforcement officials would be especially challenged by new electronic payment and information technologies. The findings reported below represent a tabulation of agreed rank orderings, together with RAND’s appraisal of the participant’s debate.

The following discussion begins with the category rankings participants agreed on as the set of issues most important to near-term policy development in coming to grips with the challenges and opportunities of emerging Cyberpayments, Internet banking, and Internet gambling industries. At the end of this discussion are the overall issue priorities reached by participants and a concluding assessment of the meaning of this broad consensus to future action in this area.

DUE DILIGENCE ISSUES

Under this heading, participants addressed each of the issues in terms of the logical sequence of activities designed to establish the fundamental responsibilities of operators of
Cyberpayments, Internet banking, and Internet gambling establishments in ensuring that criminals
did not gain access to their funds transfer and transactions processing systems to support illegal
activities. Discussions began with consideration of the potential value of one of the most salient
features of cyberspace - payer anonymity - to the criminal exploitation of electronic commerce
activities. From this early perspective their grew an intense discussion of the means available to
law enforcement and oversight authorities to mitigate the anonymity of Internet business
activities which were seen as especially prone to abuse.

A great deal of emphasis was placed on the degree to which commonality of definitions
was vital to establishing the identity and transactional characteristics of those with legitimated
rights to use Cyberpayment instruments, transact business through Internet banks, or gain access
to services through an Internet gambling establishment. It was pointed out that divergences in
national rules regarding documentary proof of authorization to transact business - that is, proof
regarding one's identity - could create significant problems for authorities seeking to create a
profile of potentially suspicious activities.

The disposition of transaction records was also the subject of debate, with one
perspective holding that Internet Gambling would inherit "real world" gambling's concern with
ensuring the complete confidentiality of gamblers' identities, because of social and legal (in some
jurisdictions) proscriptions against the activity. Those arguing this position tended to hold the
view that a direct borrowing of rules barring the disclosure of complete identifying information in
a gambling setting from the real world to cyberspace was in order. An analogy was made with an
individual walking into an establishment where slot machines were legal and playing them with
cash. No identification would be required of a player (beyond, perhaps, a proof of age in some
cases), and the player's winnings would be credited in without the necessity of showing any
customer identification at all, except for large slot and keno jackpot wins and currency transaction
reporting found in the United States.

Beyond the Internet gambling environment, however, a fair degree of consensus was
visible that held that Cyberpayments and Internet banking raised a similar set of issues relating to
the responsibilities of issuers to ensure that they were aware of the identities and transactional
characteristics of their customers. This translated into a clear consensus favoring the
development of some commonality of rules for the collection and sharing of electronic
information gained on the cyberspace transactional activities of suspected money launderers and
financial criminals. The substance of these rules was not the focus of significant discussion. It
was noted, however, that a significant privacy issue arose in some countries with respect to the
sharing of confidential economic information with a foreign jurisdiction. This issue was of
particular importance when the issue of offshore Internet banking arose, where some participants
argued that traditions of account confidentiality and record secrecy could not be compromised.

More generally, concerns were raised with public acceptance of an intrusive system of
government surveillance over ordinary electronic commerce. Not only was such a system likely
to be rejected by the public, it was argued, but also it was clear that the overwhelming quantity of
data collected would be almost useless to law enforcement in the absence of some prior clues
regarding potentially suspicious activities by individuals.

After lengthy discussion of these issues a broad consensus arose on the following listing of issue
priorities:

1. Know Your Customer Issues - Developing international norms for cyberspace "Know Your
   Customer" rules and regulations.
2. Identification Issues - Employing digital signatures and encryption to establish a safe and secure infrastructure for the authentication of digital transmissions in Internet gambling, Internet banking, and Cyberpayment applications.

3. Establishing an information system to enhance the investigation of cyberspace financial crime.

OVERSIGHT AND SUPERVISION

Discussions on this topic focused on the primacy of licensing in the effective exercise of oversight in Cyberpayments, Internet banking, and Internet gambling. Licensing criteria were viewed as a significant potential multiplier on the effectiveness of other measures against fraud and abuse in operating commercial entities. One point that recurred in these discussions was that the licensing dilemma - not wanting to place too onerous a burden on legitimate operators while wishing to deter potentially illicit entities from operating - was similar in the physical and cyberspace worlds.

A perspective was also offered that held that different countries had reached divergent conclusions regarding how to go about conducting investigations of persons and entities seeking to gain a license to operate banking and gambling establishments in CFATF jurisdictions. In the cyberspace context, licensing was seen as especially critical because of the crossborder nature of many of the services delivered through the network. One argument that emerged in the discussions held that jurisdictions with a strong commitment to rigorous and effective oversight of their operators of potential Internet banks and gambling establishments could be "held hostage" by the weak enforcement and oversight policies of their neighbors. The "cascading downward" of regulatory coverage triggered by weak enforcement in any single jurisdiction was argued to be worse in cyberspace but hardly a unique problem.

Another important element of any system of oversight and supervision was held to be the collection of records and investigative techniques regarding suspicious patterns of transactional activity. On this issue, cyberspace was argued to present a unique series of challenges because the legal status of transaction records was unclear in a number of the jurisdictions represented at the exercise. Added to this fact was the potential problem of how to share information across international borders. A number of participants noted that evidence obtained in a neighboring jurisdiction would not necessarily be admissible in their courts.

The role of inspection in maintaining the integrity of the oversight and supervision function was also the subject of considerable comment. On the issue of how to execute "on-site" inspections of Internet banking and Internet gambling establishments, it was broadly acknowledged that new technological means would likely be required to execute effective auditing and record analysis functions.

One perspective offered by participants held that the state where one of a potential multiplicity of Internet banking or gambling establishment's servers was located should exercise oversight and supervision responsibilities over the involved commercial entity. Another perspective countered by saying that in the current environment a branch operation of an international financial institution was examined by its home government's oversight authorities. It was further argued that this sort of quid pro quo allowed less resource-rich jurisdictions to obtain access to advanced auditing and investigation techniques that they would otherwise be unable to afford - thus further enhancing the safety and soundness of financial institutions operating in less developed jurisdictions.
Irrespective of the advantages accruing to these locales, a counter-argument was made regarding the potential impairments to sovereignty that could result if smaller jurisdictions did not obtain independent capabilities to perform these duties - especially given the growth of Internet banking and gambling establishments in the Caribbean region.

Mandatory filings of transactional data by Cyberpayment, Internet banks, and Internet gambling operators was frequently mentioned as a means of leveraging the relative underdevelopment of some state’s oversight and supervision capabilities in electronic commerce. Privacy concerns arose as a point of contention on this subject, with perspectives argued on both sides of the question. Some participants apparently felt that the collection of electronic information on “potentially suspicious” transactions posed a “Big Brother” threat to civil liberties. Those arguing this position also offered the opinion that their publics would never tolerate a very intrusive system of record keeping on legitimate transactional activities. Others argued a slightly different position, holding that the collection of broad transactional data was neither feasible nor desirable.

The concern with overloading still embryonic systems of information management with a potential flood of new transaction records was said to argue for a more discriminating collection of information thought to represent a “trigger,” or advanced indicator, of suspicious activity. The design of these triggers in Cyberpayment, Internet banking, and Internet gambling venues was seen as a subject that warranted considerable international discussion.

Overall, the issue priorities for participants in the category of Oversight and Supervision were

1. Licensing - Establishing rules governing permissible operators of Internet gambling, banking, and cyberpayment systems.
2. Transaction Thresholds - Development of international norms on record keeping threshold triggers for cyberspace funds transfers and transactions.
3. Oversight and jurisdiction questions concerning international cyberspace financial services operations.
4. Techniques for “on-site” inspection in cyberspace.

LAW ENFORCEMENT ISSUES

The debate on law enforcement issues followed the pattern of the discussions on due diligence and oversight and supervision in its focus on the critical factors that differentiated cyberspace from the physical environment. Established rules governing privacy were seen as key to the allowable latitude that law enforcement would be afforded in investigations of suspicious activity in electronic commerce. It is in this area that the unique technological characteristics of information networks came to the fore. Participants seemed especially aware of the challenge facing law enforcement in the tracking of funds flows and account activity in an environment where distance was losing more of its meaning every day.

Adaptation of law enforcement techniques to address new technological challenges was seen as critical to the maintenance of investigative capabilities in the new environment. The application of new information technologies to law enforcement was seen as critical to the maintenance of effective investigative capabilities.
Among the techniques discussed in the exercise and among participants were digital signatures and biometric identification, network traffic analysis devices, and authentication schemes for online transactions processing. It quickly became apparent, however, that prior legal issues needed to be settled in parallel with the adoption of potentially promising technologies that could make contributions to investigative effectiveness.

Establishing a legal regime under which law enforcement could gain access to electronic commerce transaction records was a key point emphasized by many participants. An intense debate on this subject focused on the question of whether unique “probable cause” requirements would hold for access to records deriving from cyberspace economic activities or whether such records would receive the same protections accorded to more traditional records of personal economic activities. Those arguing against special access requirements for electronic commerce transaction records pointed out that most jurisdictions already had laws and regulations governing law enforcement access to financial records in the context of a criminal investigation. From this perspective, a simple extension of these rules would allow for the handling of electronic records in ways analogous to the management of more traditional physical evidence. A strong counter argument was made by others who noted that some jurisdictions did not allow the use of electronic evidence from wiretaps to be introduced into a criminal trial. Those arguing this perspective maintained that new laws would be required to manage the introduction and evaluation of electronic evidence in cases of suspected cyberspace money laundering or financial fraud.

At the same time it was generally agreed that the admissibility of electronic records from Cyberpayment, Internet banking, and Internet gambling venues was inherently intertwined with the issue of which investigative techniques law enforcement would be able to use to gain independent corroboration of initial suspicions of wrongdoing. If laws governing the admissibility of evidence denied the availability of electronic transaction records obtained through the application of advanced surveillance and computing techniques, little would be gained by investing in the new information systems and skills most observers consider to be critical in governmental management of electronic commerce problems.

The debate thus focused on the legal regime within which electronic evidence and sophisticated computer-based investigative tools and techniques could both be applied in support of criminal investigations and eventual prosecutions. The issue area priorities for participants in this category were:

1. Establishing privacy and law enforcement access to cyberspace financial records.
2. Employing tools and techniques for intercepting communications over computer networks.
3. Determining the role of mandatory filings in combating cyberspace financial crime.
4. Determining the role of confidential informants in investigating cyberspace financial crime.

LEGAL ISSUES

The legal environment governing cyberspace was a recurring and dominant theme throughout participant deliberations during the exercise. As is evident from the narrative discussion above, legal constraints on technical and economic possibilities were seen as critical to achieving an appropriate balance between the safety and security of the economic environment on the one hand, and the innovation and growth potential of electronic commerce on the other. Discussion of legal issues focused on the domestic and international elements of the legal regime.
that would be necessary to contain potential abuses of Cyberpayments, Internet banking, and Internet gambling.

It was noted above that law governing electronic commerce activities in one jurisdiction could be nullified by a contrary legal situation in a neighboring country. Mitigating negative effects flowing from divergences in legal proscriptions was a central theme in participant discussions. An early consensus emerged on the necessity for some form of commonality or at least complementarity regarding definitions of cyberspace crime in different jurisdictions. Interpretations of criminal behavior in electronic commerce would naturally be expected to grow out of existing legal traditions. Here it was observed that existing differences regarding permissible economic activities already impede investigations of suspicious activities. Cyberspace has the potential to exacerbate these difficulties further by diminishing considerably the importance of international borders to the occurrence of financial crime.

As we saw under the last heading, ensuring the admissibility of computer-based records in a criminal court is central to the effective prosecution of criminal activity in the electronic commerce setting. It was observed repeatedly, however, that many jurisdictions lack legislation to permit wiretapping of telephone lines in pursuit of a criminal investigation. Many participants saw this observation as symptomatic of how much progress still had to be made before a successful legal response could be designed to address electronic commerce challenges.

One danger identified by many participants from smaller jurisdictions was the impact of extra-territorial applications of national laws from larger jurisdictions to activities that took place in the Caribbean and elsewhere. These participants asserted the right of smaller jurisdictions to draft their own laws regarding electronic commerce, and voiced strong objections to any formulation of international legal responses that coerced them into adopting a foreign legal interpretation of electronic commerce activities. Indeed, this assertion of independence regarding the appropriate legal treatment of Cyberpayments, Internet banking, and Internet gambling enterprises focused attention on the belief of many exercise participants that the legitimate economic activities flowing from the emergence of electronic commerce promise significant wealth creation opportunities for developing countries. In this context, many jurisdictions are loath to adopt a legal framework for the oversight of electronic commerce that may be perceived as inimical to their medium- and long-term economic prospects.

In a related area, participants discussed how the “appropriate” investigating prosecutorial jurisdiction for a crime in cyberspace was to be determined. A concern was voiced that conflicts over jurisdictions in criminal cases involving electronic commerce could allow criminals to avoid prosecution. In turn, in cases of collaborative regulatory and law enforcement action prosecutorial “appropriateness” could be construed to mean the jurisdiction with the laws most favorable to a successful prosecution of wrongdoers. Participants generally concluded that a dialogue between jurisdictions on this topic would be necessary to ensure that adequate coordination of efforts was achieved.

Overall, the issue priorities for participants in this category were

1. Establishing comparable laws and regulations governing cyberspace financial crime.
2. Exploring extra-territorial issues and the determination of appropriate jurisdictions in the investigation and prosecution of cyberspace crime.
3. Determining the admissibility of computer records in international cybercrime investigations
4. Seeking common definitions of “legitimate” and “illegitimate” cyberspace financial activity.
OVERALL RANK ORDERED ISSUE PRIORITIES

After discussing the individual categories of issues participants were asked for their overarching issue priorities. This list includes those areas where future policy development is most critical to coming to grips with potential abuses of Cyberpayments, Internet banking, and Internet gambling products and services. A high degree of consensus was achieved, though unanimity on approaches to actually addressing the issues raised was not present:

1. Legal Issues - Establishing comparable laws and regulations governing cyberspace financial crime.

2. Oversight and Supervision/Licensing - Establishing rules governing permissible operators of Internet gambling, Internet banking, and Cyberpayment establishments.

3. Due Diligence/Know Your Customer Issues - Developing international norms for cyberspace "Know Your Customer" measures and procedures.

These three issues encompass the broad spectrum of issues raised by the emergence of electronic commerce. Participants concluded that the establishment of a common legal framework governing electronic commerce is the critical first step in coming to grips with a genuinely international phenomenon that will affect all countries. Participants concluded that, once work was begun on establishing a common legal framework, consistent licensing of the operators of Cyberpayment, Internet banking, and Internet gambling establishments was necessary to minimize cross-border problems triggered by "rogue" operators who sought to utilize the "weakest link" phenomenon to exploit weaknesses in electronic commerce oversight.

Finally, participants concluded that entities operating electronic commerce enterprises that delivered services within their jurisdictions should be required to show due diligence in the way they establish the integrity and legitimacy of customers transacting business through their computerized infrastructures. In this way, operators become a crucial adjunct to government oversight authorities in making sure that patterns of abuse in electronic commerce do not go undetected for a significant period of time and that companies offering financial services on the Internet do so in ways that protect the integrity and soundness of payment systems around the world.

The Step Three exercise deliberations formed the immediate backdrop for the in-depth discussion of the impact of electronic commerce on Caribbean jurisdictions that constituted the second half of the May 1998 CFATF/ComSec workshop. In this workshop CFATF and Commonwealth government officials from North America, Europe, and the Caribbean undertook to prioritize the elements of a work plan and research agenda on Cyberpayments, Internet banking, and Internet gambling for the two organizations' secretariats. These deliberations produced the conclusions and recommendations paper provided in Appendix B of this report.
9. CONCLUSIONS

RAND's analysis of the exercise deliberations yielded a number of important themes and concepts of continuing utility to future analysts and decisionmakers concerned with cyberspace-based payment systems. Our analysis focused on four issues that taken together constitute the central challenge that Cyberpayments, Internet gambling, and Internet banking pose to established governmental modes of oversight. These challenges are (a) the potential rise of a new kind of cyberspace-based criminal enterprise; (b) the problem of jurisdiction in cyberspace, twinned with ambiguities regarding the evidentiary status of electronic data, labeled "Type A Failure"; (c) the potential failure of traditional investigative tools and techniques, labeled "Type B Failure;" and (d) the potential promise of information technologies as positive contributors to government oversight, regulatory, and law enforcement capabilities. The next section outlines each of these subjects in greater detail.

THE RISE OF A NEW CONCEPTUAL MODEL OF CYBERSPACE CRIMINAL ENTERPRISE

Central to the exercise scenario was a hypothetical international criminal organization able to exploit the technologies of the global information infrastructure (GII) to conceal its activities from government authorities. The organization - the daGama family - used legitimate business activities in banking and financial services, and in the tourism, trading, and gambling industries, operating principally in the Caribbean, to conceal money laundering and narcotics trafficking. While set in a hypothetical future, this criminal organization was itself a direct extrapolation of existing international criminal enterprises. It is a truism among law enforcement authorities that narcotics cartels and other sophisticated organized crime groups are early adopters of advanced technologies. This pattern was earlier indicated by these groups' adoption of personal computers, pagers, and cellular telephones to facilitate their criminal activities.

With this background, what is one to anticipate regarding potential criminal use of cyberspace? Beyond the current concern with hackers invading private and governmental computing facilities, the emergence of Cyberpayments, the rise of Internet banking, and the emergence of Internet gambling may pose unavoidably attractive targets for criminal exploitation. This reality was explored at length in the exercise scenario, with a number of examples of potential criminal exploitation of electronic commerce products and services outlined in the supporting future history and substantive narratives. Participants uniformly agreed that these means of exploitation would pose significant challenges to their existing arsenal of investigative tools and techniques.

The exercise also conceptualized a hypothetical multinational Western Hemisphere law enforcement and regulatory response to the da Gama family and comparable criminal enterprises - the Permanent Joint Task Force (PJTF). This mechanism was designed to facilitate information sharing, collaborative investigations, and complementary prosecutions. As many participants observed, such a multinational structure, possessing operational responsibilities and authorities, does not exist at present anywhere in the world, and would by itself represent a major breakthrough in international governmental cooperation. These same participants also acknowledged, however, that such a response would be insufficient without parallel changes in national regulatory and law enforcement frameworks governing cyberspace. Clearly, coordinated national and international joint policy development are key to effective oversight.
Type A Failure: The Problem of Jurisdiction in Cyberspace. It is possible that, even if law enforcement authorities think that they know "how" a cyberspace crime is being committed, evidence supporting that conclusion may be inadmissible in courts because of a lack of an adequate legal framework. Existing laws appropriate to effective oversight of traditional money laundering, fraud, and financial crime may prove inadequate if they are not adapted - or made adaptable - to keep pace with the new electronic commerce setting.

Controversies regarding the relevant jurisdiction for investigating or prosecuting cyberspace crime may also arise from the fact that electronic commerce is developing much more rapidly than the legal framework that will contain it. In addition, many jurisdictions already lack legislation allowing the use of traditional wiretaps and evidence obtained from wiretaps.

How are states to collaborate in the investigations of cyberspace crime? Existing methods of law enforcement and prosecutorial collaboration will need to be reinforced by the further development of legal and evidentiary rules that allow the introduction and utilization of information derived from computers and the Internet in investigations and subsequent prosecutions. This activity will require that law enforcement and legal authorities gain a greater understanding of the architecture and modes of utilization of the current and future Internet and of potential patterns of abuse that might develop in that environment. Without responsive, collaborative development of these laws criminals could creatively exploit differences in legal regimes to avoid prosecution for cyberspace crime.

Type B Failure: The Potential Failure of Traditional Investigative Tools and Techniques. Traditional investigative tools and techniques used by law enforcement to trace money laundering rely on the availability of paper-based records held by regulated financial institutions. These records create a "paper trail" linking an individual to a movement of funds and to potentially useful information or evidence. Anything that interferes with the creation of this paper trail has the potential to seriously impede such law enforcement investigations, perhaps creating a critical gap in evidentiary development.

The Internet, and the associated electronic payment technologies explored in the exercise, have inherent characteristics which create the potential for serious weakening of existing law enforcement tools and techniques. Some examples will help to reinforce this situation: commercially available secure telephones with encrypted communications capabilities may confound established modes of law enforcement wiretaps; the encrypted transmission of financial transactions over the Internet may deny law enforcement its primary traditional means of tracking flows of funds - auditable financial records; Internet gambling applications might employ pseudo-random number generators to "tilt" games in favor of the gambling operator. As an example of the challenge to law enforcement, in the latter case detection of such a fraudulent game could require considerable expertise in computer-based algorithm design, something most law enforcement entities do not possess.

The Promise of Information Technologies. On the more positive side, information technologies may offer new capabilities for governments in overseeing electronic commerce and may make unique contributions to the investigation and prosecution of other types of crime. Criminal exploitation of electronic commerce is necessarily rendered more difficult if e-commerce products and services are "hardened" against fraud and abuse through the deployment of protective tools and techniques. Advanced action by service providers has the potential to reduce fraud on the Internet, thus making law enforcement's job that much more manageable.
Three areas of development may make key contributions in this domain: Record Keeping Systems, Authentication Measures, and Tracking Systems.

Record Keeping Systems

Electronic record keeping of commercial transactions on the Internet presents a potentially lucrative data source for law enforcement and governmental regulators. Record keeping systems typically collect information on the nature of network traffic, allowing network managers to characterize broad trends in user access. Such systems typically collect their information through the creation of a set of server logs that record the time of an online transaction, the duration of an online session, and information relating to the network address of the consumer or business initiating the transaction. Network logs of this type can underpin more sophisticated analysis of network traffic through a suite of “profiling techniques,” whereby artificial intelligence techniques are used to detect patterns of transaction activities associated with money laundering or cyberspace financial crime.

Analysis of network traffic is one quick means of gaining a broad appreciation of the structure and timing of electronic commerce. It allows companies to “narrowcast” their products to particular customers according to their likely interest in purchasing items and creates new information when databases of customer transactions are compared to information from credit reports and online directories. “Data mining” of consumer transactional data is a set of techniques used to find associations between consumer transactional behavior and credit worthiness and other demographic data of interest to marketers. Data mining is performed by statistical software packages installed on high-powered computer work stations. Comparable analytical tools may also be of use to law enforcement authorities and regulators to discern patterns in transactional data associated with criminal activity.

Authentication Measures

Authentication measures allow network operators and government authorities to identify individuals or entities involved in cyberspace-based financial activity. A number of technologies are key to this capability:

Digital Signatures - a label attached to e-mail, data, or electronic value flowing within a network that authenticates the identities of particular individuals or entities. When tied to particular transactions, digital signatures create an electronic trail, linking online transactions with particular individuals.

Biometric Forms of Identification - hardware and software systems that authenticate the identities of human beings through the electronic capture of unique data characterizing a person’s features. Examples include images of a person’s fingerprint or palm print, a laser-scan of an individual’s retina or iris, and a voiceprint.

The combination of record keeping systems and authentication measures could yield an infrastructure of potentially great utility to law enforcement and government regulators in establishing the money/illicit activity nexus so important to the building of a case for potential prosecution.
Tracking Systems

Network tracking systems are, perhaps, the most experimental of all the techniques becoming available for conducting surveillance over online activities. Still in research are techniques deriving from already deployed artificial intelligence (AI) applications that use knowledge-based systems to characterize network traffic according to such criteria as point of origin, duration of online session, and identity of the user. The major difference with these techniques is that they are implemented in software analogous to that of a computer virus.

Network-borne tracking systems are of two broad types: classifier systems, using rule-based models derived from the judgement of human experts to categorize online traffic; and software agents with elementary machine “learning” capabilities that are reinforced by continual exposure to transaction data in a network setting.

Each of these tools has the potential to conduct partially or completely autonomous data-gathering activities - in some sense analogous to motion or temperature sensors in the physical world. Development of these tools is at the speculative “outer edge” of research, and their true potential for intercepting potentially suspicious electronic commerce activity remains to be demonstrated.

Electronic traces of online activity raise concerns regarding consumer privacy and potentially inappropriate uses of sensitive information by unauthorized persons. It is important then to consider these techniques in relation to the regulatory and law enforcement purposes they may support. It is nonetheless true that the electronic infrastructure to perform many of these activities will likely emerge as a consequence of the growth of electronic commerce.

Entities providing funds, goods, and services over the net are necessarily concerned with ensuring the safety and security of their transaction systems from compromise by hackers or thieves. In turn, network providers of financial services must meet established safety and soundness concerns relating to their ability to identify customers. Each of these concerns means that some sort of authentication, tracking, and record-keeping infrastructure will likely emerge from the electronic commerce arena as a result of market forces.

IMPLICATIONS

Taken together, the challenges described above raise many questions regarding the continuing ability of governments to maintain, and/or sustain progress toward existing anti money laundering and anti-financial crime objectives. Existing institutions simply are not yet designed to manage emerging cyberspace technologies or respond to the potentially serious impact these systems could have on the investigation and prosecution of organized crime.

A coordinated international response to the full spectrum of these problems seems an appropriate place to begin. Crafting and successfully marketing such a strategy to protect the security and integrity of cyberspace-based financial activity now and in the twenty first century should be an imperative of all those interested in the growth of this new medium.

The results of the CFATF/ComSec work shop on Money Laundering Through Emerging Cyberspace Technologies (Appendix B) represent an important step - the first structured international attempt to come to grips with this complex set of challenges. Moving forward with policy development initiatives would provide concrete evidence of a serious international effort in

55
this new arena. It would also provide an opportunity to exploit the emerging international consensus that cyberspace be taken seriously as both a technological challenge, and a legal, administrative, and cultural challenge to traditional modes of economic and regulatory governance.
The Emergence of Electronic Commerce

As the twentieth century came to an end the basic technologies were in place to facilitate the rapid expansion of electronic commerce in both business-to-business activity, and in the marketing of consumer goods over the Internet. The Secure Electronic Transaction (SET) encryption standard was now widely adopted by the electronic commerce community, allowing a heightened level of security for Internet-based financial transactions and giving electronic commerce a significant boost as it helped to allay consumer fears that personal financial data, when transmitted via the Internet, would be vulnerable to theft and/or misuse.

The Maturing of Cyberpayments

By 2001, technical compatibility among most major competing Cyberpayment products was achieved as common physical and electronic architectures for the instruments met international standards. Debate on the economic viability of these new electronic products was rendered largely moot by the broad deployment of multi-use smart cards containing microprocessors capable of: (1) delivering multiple services to the user including stored value, debit, and credit elements and (2) serving as a personal “data haven” for security access codes, medical records, and other sensitive information.

As the new generation of smart cards was deployed, the retail industry was retooled with multi-use payment terminals through a special replacement program begun in early 2001 by a consortia of Cyberpayment providers in conjunction with their banking partners. The low cost buy-back program quickly created a critical mass of retailers able to participate in electronic commerce.

The continuing expansion in Internet bandwidth (a quadrupling in data throughput capacity between 2000 and 2002) meant that the services made available by these products could be delivered at increasingly greater distances and with enhanced rapidity.
Even as these products were achieving global acceptance, however, many nations continued to struggle with key regulatory questions. In most countries, authorities followed a slow and cautious path, not wanting to upset the continued growth of e-commerce.

The Maturing of Internet Banking

By the end of 2001, many existing brick and mortar banks were offering basic services on the Internet, providing an increasingly popular alternative to the still available branch bank. At the same time, however, many new banks were opening exclusively for business on the Internet. In this context, a whole new sector of offshore Internet banks also began to appear.

The types of Internet banking services provided varied between financial institutions. While most of the established banks were offering the same banking products via the Internet that were available through a branch location (such as checking and savings accounts, personal loans, and money market investments), many of the offshore Internet banks offered a greater range of services, akin to those formerly only available at large bank offices or private banks. These included the issuance of high denomination Cyberpayment instruments, currency exchanges in near-real time transactions, and enhanced account secrecy.

By late 2001, it was estimated that 25% of consumer banking activity and 60% of business banking activity was being conducted via the Internet with 30% of the on-line activity passing through offshore banks.

Internet banks in some countries remained subject to traditional oversight by banking regulators. The problem remained, however, that different jurisdictions had varying rules regarding the operators of Internet banks and on the oversight rules governing these entities.

In addition, traditional banking community “know your customer” means for gaining early detection of potentially suspicious financial activity were faced with progressive obsolescence as Internet delivery of banking services partially replaced more traditional financial transactions.
The Maturing of Internet Gambling

Shortly after the turn of the century Internet gambling operators and smaller ISPs began to combine to form Internet-based financial services entities in order to compete with larger organizations. In turn, these financial services entities contracted with computing and telecommunications companies in order to deliver “premium” services over the Internet including:

- Enhanced confidentiality and security of financial funds flow information.
- Structuring of financial transactions to minimize regulatory and tax exposure.
- Issuance of “high denomination” Cyberpayment instruments with hybridized features including access to:
  - Money market accounts,
  - Holdings at Internet casinos,
  - On-line currency exchange and arbitrage,
  - Real-time balance transfer facilities for accounts in different Internet financial institutions.

Individually these features were troubling but not necessarily illegal in nature. However, as the number of individuals availing themselves of these “premium” services increased, by 2001 many governments were becoming increasingly concerned with the potential for fraud, money laundering, and, in some jurisdictions, tax evasion and other tax issues.

One aspect of Internet gambling that especially troubled regulators was the potential for entities in foreign jurisdictions to offer gambling services to customers in geographic locales where the particular products or services were illegal. More narrowly, however, new difficulties of oversight were seen to flow from the primarily electronic nature of the gambling itself. Issues of record-keeping, auditing by financial examiners, and the permissible owner/operators of Internet gambling establishments all were complicated by the cross-border nature of the industry.

By 2001, the number of Internet-based Casinos had increased dramatically to more than 250 globally. Many of these institutions operated in offshore and “tax friendly” jurisdictions, and many had formed cooperative partnerships with offshore banking entities.

In 2002 headline news stories reported that the total amount wagered in the U.S. and internationally on the Super Bowl via Internet gambling - an estimated $40 billion - exceeded that wagered on the game in all (other) legal U.S. gambling sites combined.
Growth in Cyberspace Criminal Activity and Organizational and Institutional Responses

Predictably, criminal organizations were quick to perceive the opportunities made available by the new global networks.

Cyberspace crime during most of 1990s consisted largely of hacker intrusions into computer networks and of piracy affecting expensive business software applications. However, by 2000 law enforcement and oversight authorities were seeing an increasingly large number of large-scale thefts of credit card and other consumer purchasing data and of proprietary information - plus occasional attempts to extort funds based on the threat to disrupt key network resources.

By 2001, new challenges to law enforcement and oversight authorities were emerging, many clustered around the cross-jurisdiction implications of electronic commerce and its subsidiary elements of Internet gambling, Cyberpayments, and Internet banking.

Discussions on international coordination of oversight rules applying to Internet banking, Internet gambling, and Cyberpayments began in 1996 in the G-7 Financial Action Task Force (FATF) and Caribbean Financial Action Task Force (CFATF) typologies meetings with coordinated action initially confined to establishing common guidelines for the investigation and prosecution of cyberspace-based financial crime.

However, as the number of links between networks expanded and the scope of Internet crime increased, existing levels of coordination were found wanting. Rules governing one country’s financial institutions were frequently contradicted by those of its neighbors. Disagreements - or at least variations - were frequently found in the following areas:

- Regulations pertaining to the issuance of Cyberpayment value
- Oversight rules governing permissible ownership and operation of Internet banks
- Technical rules governing Internet gambling
- Statutes pertaining to the criminal prosecutions of Internet crime
The increased involvement of organized criminal entities in Internet-based financial crime further exacerbated oversight problems. By 2002, increasingly complex money laundering strategies were observed as the electronic economy continued to expand.

In the period from 2000 to 2002 an escalating series of cyberspace crimes helped to focus attention on the potential magnitude of the emerging problem:

**In St. Kitts**

In March of 2000, the collapse of the Global Funds Future Bank in St. Kitts provided a second example (after the collapse of the European Union Bank in Antigua in 1997) of some of the new dangers flowing from Internet banking. Depositors lost funds as the owner/operators of the bank - apparently criminals from Nigeria - fled with the bank’s holdings. While arrests were made, depositors were unable to recover any of their funds, estimated at over $250 million, from the bank. This case raised serious issues regarding the strength of bank oversight in various jurisdictions.

A similar occurrence in July of 2000 in the Cayman Islands underlined the seriousness of shortfalls in Internet banking oversight rules.

**In Kansas City**

In November 2000, a fraud scheme on a commercial web site was broken up by the U.S. Secret Service and the IRS. The scheme consisted of the deliberate over-billing of consumer accounts when on-line purchases were made. Charges to stored value, credit and debit cards were increased by 2-5 per cent, depending on the transaction, with the incremental difference transferred to accounts controlled by the owners of the on-line firm. Because of the volume of transactions on this site (which sold books and magazine subscriptions) the theft went undetected for a considerable length of time.

The scheme was discovered by IRS auditors who received a tip that the company was understating its annual business volume. Initial estimates of the illegal profits derived from the scheme totaled over $10 million.

**In Toronto**

In early 2001, a two-year scheme involving over-billing for airplane tickets ordered over the Internet was exposed by an undercover operation run by the Royal Canadian Mounted Police (RCMP).

The scheme employed a deliberately introduced flaw in a database management system containing near “real time” ticket price quotes. The software employed by the perpetrators systematically over-stated ticket prices to consumers, with the difference between the quoted price and the real price (4 to 6 percent) being diverted into hidden accounts. Because of the fraud involved and the scope of the injury to thousands of affected passengers (millions of dollars), the perpetrators received stiff prison terms.
In Lisbon

In a scheme uncovered in Lisbon in mid-2001 software written to enable on-line banking for account holders at a number of major banks was surreptitiously modified to order the unauthorized transfers of funds from consumer accounts to secret numbered accounts in third party financial institutions.

Because a number of banks shared a common software base for their consumer-level account access products, the scheme was successful in stealing funds from over 5000 people, and was in place for well over a year.

To launder the stolen funds, the perpetrators utilized disintermediated value transfers from Internet Banks to stored value smart cards. Eventually over $25 million was transferred within cyberspace through a complex layering operation designed to conceal the true origins of the funds. Investigators followed leads on funds sent to Germany and Luxembourg, but authorities in those jurisdictions lost the trails in cyberspace.

When the scheme was finally discovered only a small number of people were successfully prosecuted for the thefts. The bulk of the funds involved were never recovered.

In Rome

During a 2002 investigation of drug money laundering, Italian law enforcement officials discovered a troubling pattern of funds transfers from Rome-based accounts to offshore banks tied closely to known drug cartel principals. On closer examination a sophisticated scheme was discovered that used Internet banks, Cyberpayments, and a casino to launder illicit funds. The criminal activity worked in the following manner:

1. Funds were transferred from a bank account in Rome to the Internet bank.
2. A large initial balance was established in an account at an Internet bank.
3. The account was connected to a stored value smart card denominated to maintain balances as high as $50,000.
4. At regular intervals funds were transferred from the smart card and sent to an account at a second Internet bank registered in a foreign jurisdiction.
5. Simultaneously, funds transfers from the first Internet bank account were initiated into the Cyberpayment instrument, allowing the balance to remain unchanged.

Money Laundering - Basics

Money laundering is a process through which criminal proceeds take on the outward appearance of legitimacy. The process has three principal components:

- **Placement** of illegally generated funds into the financial system.
- **Layering** to obscure the illicit origins of funds by the careful structuring of transfers to impede potential investigation.
- **Integration** of funds from illicit sources with legitimate funds as they enter the mainstream economy.

Without an audit trail constructed during the placement and layering stages it is very difficult to detect illicit funds. (See Tab K - Money Laundering)
6. Within the same business day transfers were initiated from the second Internet bank into the account maintained at the first Internet bank. Scaled as equal and opposite transactions (credit and debit operations), these transfers would appear as arbitrage designed to move funds to areas of high interest/yield from places of lower yields. In fact, the funds from the Cyberpayment instrument and the second Internet bank were actually the proceeds of illegal activities - illicit gambling remittances and drug trafficking profits - laundered through an apparent cash management system maintained on behalf of a wealthy individual.

Creation of the Western Hemisphere Permanent Joint Task Force (PJTF)

In early 2003, CARICOM and the Organization of American States (OAS), supported by the CFATF and the Commonwealth Secretariat, proposed the creation of a multinational entity to address the growing problem of Internet-based financial crime. In July 2003, a Permanent Joint Task Force (PJTF) was established through the multi-lateral "Treaty of Santiago," signed and ratified by 48 Western Hemisphere nations.

The PJTF has a broad charter to develop and implement policy on a multinational basis. The PJTF also has a mandate to coordinate, oversee, and participate in multi-lateral investigations with member nations.

The PJTF is headquartered in San Jose, Costa Rica. The organization has a twelve-member Steering Committee and a six member Advisory Board – both composed of member state attorney generals and/or heads of Justice Ministries.

On a day-to-day basis the PJTF is run by an Executive Director who heads an organization with three divisions: Analysis, Information Sharing and Coordination, and Operational Assistance. (See Figure B-1)

As the division titles suggest, the PJTF performs a number of roles under its broad mandate. This can be clearly seen in the excerpts from the "Treaty of Santiago" provided on Pages B-9 and B-10.

Personnel working for the PJTF are composed of a small core of professional staff and seconded specialists from member state law enforcement, justice and regulatory agencies.

Among the early actions taken by the PJTF were the following:

- Establishment of a secure communications network linking cognizant authorities in all PJTF countries (90% complete by the end of 2004).
- Commissioning of a study of available cyberspace tools and techniques that might be applied to the emerging money laundering problems related to Cyberpayments, Internet banking, and Internet gambling.

The potential for further expansion in the role of the PJTF is somewhat controversial. What is the correct long-term role for an international inter-governmental organization in combating international Internet financial crime? What capabilities are required for an
effective international response to organized crime? In 2005 each of these questions receives different answers, in part depending on individual perceptions of the severity of Internet crime.

Figure B-1. Permanent Joint Task Force (PJTF) Organization Chart
Excerpts from the 2003 "Treaty of Santiago" Establishing the Permanent Joint Task Force (PJTF)

Signatory Nations:
Anguilla; Antigua & Barbuda; Argentina; Aruba; the Bahamas; Barbados; Belize; Bermuda;
Bolivia; Brazil; British Virgin Islands; Canada; Cayman Islands; Chile;
Costa Rica; Cuba; Dominica; Dominican Republic; Ecuador; El Salvador;
France; French Guinees; Grenada; Guatemala; Guyana; Haiti; Honduras; Jamaica;
Martinique; Mexico; Montserrat; Netherlands, Netherlands Antilles; Nicaragua; Panama; Paraguay;
Peru; Puerto Rico; Saint Kitts & Nevis; Saint Lucia; Saint Vincent & the Grenadines; Suriname;
Trinidad & Tobago; Turks & Caicos Islands; United Kingdom; United States; Uruguay; Venezuela

Observer Organizations:
CARICOM, CFATF, Commonwealth, OAS, Interpol

Article I. Mandate of the PJTF

(i) The objectives of the PJTF shall be to identify, and respond to, emerging cyberspace-based criminal threats in the Western Hemisphere.

(ii) Because of the rapidity of cyberspace transactions and the complex challenges which this now presents to all member governments, the mandate of the PJTF shall include both policy development and operational assistance.

(iii) The PJTF shall be responsible for the development of Hemispheric-wide policies designed to combat cyberspace criminal threats, as well to provide operational and technical assistance to the competent authorities of the Hemisphere.

(iv) Such assistance shall only be rendered at the invitation and discretion of individual host governments.

Article II. Organization of the PJTF

In order that the PJTF respond to the challenges of cyberspace in the most effective and expeditious manner the PJTF will be organized as follows:

a) An Executive Director responsible for organizing and staffing and day-to-day operations of the PJTF.

b) A Steering Committee of twelve rotating PJTF members to provide guidance to the Executive Director when the PJTF is not in general session.

c) A Policy Advisory Board composed of six rotating senior level officials from Attorneys General and/or Justice Ministers, Finance Ministers and/or Central Banks to serve as advisors to the Executive Director in the conduct of his duties.
Article III. Policy Formulation and Analysis

(i) The PJTF shall function as the Hemisphere’s central focal point for the analysis of policy issues with regard to cyberspace-based criminal activities. The PJTF shall inform the competent authorities in member countries of critical developments with respect to potential or actual abuse of cyberspace by criminal elements as well as recommended measures to address identified deficiencies. The PJTF shall strive, whenever possible, to be proactive in policy development and the analysis of potential and actual criminal abuse of the cyberspace. Specific duties and responsibilities in this area include:

a) Development and analysis of hemispheric policy regarding investigative techniques and procedures for cyberspace financial systems and products.

b) Development and analysis of hemispheric policy with regard to due diligence standards for cyberspace financial systems and products.

c) Development and analysis of hemispheric policy with respect to legal requests and cooperative efforts regarding cyberspace financial systems and products.

Article IV. Operational and Technical Assistance

(i) The PJTF shall render operational and technical assistance to bolster hemispheric efforts to combat cybercrime but only with the knowledge and approval of the host government(s). To this end:

a) The PJTF shall serve as a central “focal point” for formal, ad hoc, or spontaneous inquiries from member nations, as well as other responsible non-member governments and international bodies.

b) The operational elements of the PJTF may operate multi-nationally within PJTF countries, but only at the invitation and discretion of individual host governments. Whenever possible, and with the approval of the host nation(s), operational elements will be deputized to perform legitimate law enforcement activities in the agreed upon jurisdictions.

(ii) Specific operational functions of the PJTF shall include:

a) Assist in conducting international anti-money laundering financial audit/inspections of the Hemisphere’s cyberspace-based financial and commercial enterprises.

b) Operate international investigative working groups on an ad hoc basis, as required in connection with specific investigations.

c) Provide technical assistance or expertise to cyberspace-related investigations.

d) Provide specialized operation assistance to national, regional or multilateral authorities.

e) Provide a forum for the exchange of information relating to criminal abuse of the Hemisphere’s cybersystems.

f) Conduct research and development activities to create more effective law enforcement and regulatory tools and techniques to combat cyberspace crime.
Second Generation Cyberspace - Global Coverage with High Band Width

The full maturity of Cyberpayments, Internet banking, and Internet gambling arrived with the expansion in the physical capabilities of the Internet - achieved in the period 2002-2004. In this time frame, as a result of the deployment of a wide variety of ground and space-based network systems, the speed of available network links rose by a factor of 100 compared to the land line and space-based systems available in the late 1990s.

The key technological advances included cable modem technologies, advanced digital subscriber line (ADSL) technologies, asynchronous transfer mode (ATM) network infrastructures, integrated services digital network (ISDN), the replacement of old copper wire infrastructure with newer fiber network links, and the completion of a new generation of space systems such as Teledesic and Iridium which delivered high speed Internet access to most areas of the world.

By 2004, speeds of up to 2 million bits per second (Mbps) became common as Internet Service Providers (ISPs) began to contract with satellite bandwidth wholesalers to deliver premium services to subscribers. New fiber links in undersea cables also added to the available bandwidth for electronic commerce. By 2004, the previous environment of bandwidth scarcity began to be replaced by one of abundance where network operators actively sought opportunities to provide new services and products to exploit the emerging surplus capacity.

This abundance of network capacity caused the price of network access to plummet - further engendering a consolidation of the ISP tier of the networking industry. By 2004, nine global network providers of telecommunications, computing, and financial services were the source of over 80 per cent of wholesale bandwidth on the Internet.

Countries with poor telecommunications infrastructures increasingly saw this new global cyberspace infrastructure as a critical tool for economic growth and prosperity. In many cases, establishing links to this infrastructure became a national priority, removing what had seemed to be insuperable bureaucratic and regulatory barriers to network access. In addition, further expansion in the coverage of space-based wireless communications networks expanded the reach of the Internet into the few remaining areas where economics or politics inhibited its spread.

This rapidly expanding electronic commerce environment also led to technical and procedural changes in the financial services industry, in particular the establishment of a wholly new set of tools and techniques for customers.

Most important among these tools and techniques was the development of an infrastructure of digital signatures that allowed businesses to know the identity of the consumer with whom they entered a commercial relationship. These digital signatures were based on a Public Key Encryption system, whereby each consumer (and business) involved in a financial transaction authenticated - through the use of a unique private key - its rights to initiate funds flows and services delivery over the Internet. In turn, the public key made available to the other side of an Internet transaction could only be used to decrypt messages encrypted by the secret private key of the creator.
Ameridergadot, to strategy,-Augon detaiis to ned an abstracto dertifigd digital sigmature aotities that issued sigmatures to persons principally and businesses on the basis of biometric data (e.g., fingerprints, retinal scans, voiceprints, etc.). Because digital signature authorities were privately owned (though they operated under legal guidelines defined by national laws) variations in the kinds of unique identifying information that was required presented some problems of harmonization between different digital signature techniques. Some agreements were achieved in this area, but there remained an increased potential for fraud because of differences among national digital signature infrastructures.

The daGama Family

The daGama family is a long-established Portuguese merchant family with extensive operations in the Caribbean, as well as elsewhere in the Americas and Europe including:

- Shipping and Shipbuilding
- Hotel, Real Estate and Civil Engineering
- Banking and Financial Services
- Telecommunications, Media, and Internet Service Provision

The parent company of these enterprises is DGA Enterprises SA. The daGama family controls its enterprises through a complicated network of holding companies and an interlocking directorship of family members on company boards. (See fold-out at the end of this Tab.) In addition, some of these companies are located in countries that are secrecy havens, as are several daGama-owned computer servers.

Since 2001, the daGamas have exploited their expertise in banking and the Internet to develop an extensive array of Internet banking and other Internet-related telecommunications and financial software products and services including:

- Commercial encryption software
- Internet banking
- Financial software development
- Telecom and ISP services
- Global Internet gambling
- Advanced gaming software
- Cyberpayment instruments specially tailored to Internet gambling

These and other daGama operations are linked into a dedicated global wide-area network using an array of leased lines, satellite and fiber-optic connections. The encryption used on this network exceeds that allowed in the U.S. but is legal in most jurisdictions in which the daGamas operate.

Among the more dynamic of the daGama enterprises is Trade Winds SA an “entertainment” subsidiary of Devertron Entertainment Group, the daGama holding company for all of its shipping interests, headquartered in the Bahamas. Trade Winds is operated by the third generation son, Don Carlos daGama, one of the leading family members. Trade Winds
began operating floating gambling casinos in the Mediterranean in 2001 and now operates a four ship fleet of Liberian-registered casino ships (with vessels in the Mediterranean, the Baltic Sea, the Black Sea, and the Caribbean Sea). Two larger ships are under construction. In addition to gambling (including Internet gambling), the ships are also active in global exchange rate arbitrage through Internet banking and Cyberpayment instruments. Of particular importance are “private banking services” conducted via highly encrypted information systems.

Rumors persist within the underground world that the daGamas run an extremely high-tech money laundering operation shielded within their massive corporate structure.
CFATF Exercise

Tab C

Exercise
STEP ONE

4-17-98  1308

5-6 May 1998
Tab C
STEP ONE Situation Report

In Kingston, Jamaica

April 10, 2005 - Undercover narcotics officers working for the Jamaican National Police reported that drug dealers in Kingston were offering 10-15% discounts to customers who paid with smart cards. The rationale given was the cost of money laundering for smart cards was “less than half that for cash and far less risky.”

Smart cards in this operation are apparently laundered through a chain of grocery stores which bank almost exclusively with Internet-based financial institutions. The cards are purportedly processed through merchant payment terminals where the funds are electronically commingled with sales revenue and then forwarded to the store’s legitimate business accounts.

The Jamaican investigators have on several occasions examined the sales receipts and payment terminal records at stores suspected of moving a high volume of drug money. In each instance, however, they were unable to identify inconsistencies or suspicious transactions since, as one investigator noted, “$25 smart card drug deals and legitimate $25 grocery purchases both appear in the transaction logs as ones and zeros.”

In response to this situation, investigators recently hired one of Kingston’s top computer programmers to conduct a forensics audit on a computer taken from a raid on a drug stash house believed to be associated with the grocery chain activity. The programmer confirmed that the computer was being used to store and transfer digital money via the Internet and identified several remote “remailer” sites that were being used to hide the path of the funds. Ultimately, however, she was unable to follow the money flows to their final destination and surmised that she would likely have the same problem even if given access to the computer network run by the grocery store chain.

In Miami

April 19 – A “walk-in” to the Miami office of the FBI offered to become a paid informant in connection with an alleged money laundering operation involving “a Coral Gables company called Transway Shipping and a Colombian criminal organization.” The source, a relatively new employee of Transway Shipping, claimed that the company is being used to smuggle currency out of the U.S. to locations throughout the Caribbean. To back up his story, he provided the

Artificial Intelligence
The same techniques that are used by hackers to gain access to networks may also be used by law enforcement to gain access to the paper trail underlying illegal financial transactions. Profiling of network traffic flows could be used to study changes in patterns as a means of differentiating criminal activity from normal business activities.
(See Tab L – Cyberspace Investigative Tools and Techniques)
FBI with a copy of a service contract outlining a 15% fee being paid to the company ostensibly for “financial management and consulting,” but in reality for shipping the cash.

The source agreed to meet with the FBI again in two weeks to provide “additional documents”, but he disappeared and a second meeting never took place.

**In the Cayman Islands**

April 20 - The 140,000 ton Liberian-registered *SS Tropical Paradise*, the newly commissioned member of the *Trade Winds SA* fleet of lavishly equipped cruise ships, arrived in Grand Cayman to begin its inaugural tour of the Caribbean.

The arrival of *Trade Winds*’ newest “pleasure dome” was given extensive play by the local media. TV and newspaper coverage featured the four daGama brothers and sisters who were representing *Trade Winds*’ parent corporation, *Devertron Entertainment Group*, and hosting the ship’s opening night in the harbor - with most of Caymans’ banking, entertainment, and political elites in attendance.

---

**SS Tropical Paradise**  
**Gambling and Technical Features**

**Traditional Gambling:**
- Slot machines, roulette, blackjack, poker, and other traditional games of chance
- Sports bookmaking for professional football, soccer, baseball, basketball, and almost any other major organized sporting event worldwide

**Internet Gambling:**
- 24 hour a day, 7 days a week
- Funds accepted from debit, credit, and stored value-type financial instruments as well as from traditional money orders and wire transfers
- Available to anyone in the world with a network connection
- Dedicated and highly secure wide area network (connecting all ships in the *Trade Winds* fleet)
- Links to LEO and MEO communications satellites to provide a seamless venue for Internet gamblers
- Redundant, highly encrypted data links to ensure against technical breakdowns or other interruptions in service and guard against fraud and unauthorized network intrusions
- High bandwidth to enable over 500,000 patrons to simultaneously play games on the Internet without an interruption in service.

---

The *SS Tropical Paradise* was scheduled to sail to its “semi-permanent” port facility at Dominica after a month-long tour of the Caribbean. Press reports indicated that the Dominican government had “come to terms” with the *Trade Winds* and had agreed to provide the *Tropical Paradise* with a six-month lease of docking facilities.
In Antigua

April 30 - A local banker in Antigua warned a high-ranking member of the police department that the newly opened Investment Strategies Unlimited office seemed “fishy” to him. He noted that the new company’s publicity focused on the management of investment accounts while it “looked and acted like a bank.”

In Moscow

May 2 - British law enforcement sources reported that representatives of a Russian criminal organization operating out of Moscow and Trade Winds SA have finalized the procedures for a new cyber money laundering operation for U.S. currency that would involve Trade Winds’ cruise ships and operate through a bank in Cyprus. Under the purported plan:

- The Cypriot bank would receive customer shipments of U.S. dollars, convert them to Euros on smart cards, and then ship the smart cards to various Trade Winds’ vessels
- The ships would in turn transfer the value over the Internet to the SS Phoenicia, one of the two cruise ships owned by Trade Winds operating in the Mediterranean.
- The SS Phoenicia would then transfer these “winnings” to a Lisbon-based Internet Bank that would in turn transfer them to customer accounts in various off-shore jurisdictions.

This cyber-layering effectively severed the link between the funds and the criminal organization and offered a plausible sounding “gambling earnings” explanation for the income when and if off-shore banks inquired about the origins of transferred funds.

In Tampa

May 23 - The President of the Southern Palms Bank was arrested and charged with money laundering after advanced wiretap and Artificial Intelligence (AI) techniques uncovered an elaborate and previously unseen smart card-based money laundering scheme.

Apparently the Southern Palms Bank deposited high-value smart cards into a variety of corporate accounts and then digitally transferred the value (via mobile satellite communications links using a variety of advanced encryption methods) through a server in Antigua to a variety of off-shore accounts. The accounts were almost always either Internet casinos or Investment Strategies Unlimited and the CDL Bank in Antigua - all controlled by subsidiaries of DGA America, a daGama Lisbon-based holding company.

In Port of Spain, Trinidad

May 24 – The Director of Trinidad’s Strategic Services Agency called a special meeting of senior law enforcement officials to review information collected through a wiretap operation. The operation had netted detailed discussions between two Colombian heroin traffickers providing breakthrough information regarding an apparent “$200 million per year” money laundering operation, which utilized various daGama corporate holdings as fronts. The arrangement was described as follows:
• Couriers employed by the Colombian criminal group deliver boxes of bundled currency to Transway Shipping, a daGama-owned shipping company in Florida.
• The currency is shipped via secret compartments in containerized cargo to a Trade Winds subsidiary located in the Cayman Islands where the money is deposited in a local branch of the CDL Bank, a daGama owned bank in Portugal.
• The funds are then moved electronically via encrypted e-mail to an Internet bank in Hong Kong and transferred to Colombian cartel accounts throughout the world.
• This routing of cash from street drug sales is apparently used as many as five times per month.

On the intercepts the Colombians also discussed a special deal in which they used funds from various accounts as security for a $40 million loan in Port of Spain where the traffickers are involved in a commercial land deal to develop a new resort on the north coast of Trinidad.

In Lyon, France

May 26 - The Chief of the Financial Analysis Unit (FOPAC) at Interpol's General Secretariat was briefed on a previously unknown entity, DGA Enterprises SA. The briefing indicated that during the past eight months, FOPAC had received inquires from twelve different countries regarding the activities of companies or individuals associated with DGA Enterprises. All of the inquires reflected preliminary investigative activity. Two days later FOPAC issued an advisory bulletin asking that "all member nations with information pertaining to DGA, or the Lisbon-based daGama family please respond through normal Interpol channels."

Off Cuba

May 28 - The SS Golden Coral, a container ship owned by Transway Shipping, was seized off the northern coast of Cuba by the U.S. Coast Guard cutter, Badger. Based upon information from the DEA and the use of a new generation of chemical sensors, the boarding party was able to find several large bundles of cash with a total worth of over $20 million dollars.

In Miami

May 29 - The American legal firm representing Transway Shipping denounced "U.S. military harassment" in the seizing of the SS Golden Coral and denied that its client had any knowledge of contraband on board the ship.

In Dominica

May 30 - With great fanfare, the local media announced that Trade Winds SA was offering several hundred jobs and also making a "donation" of $50,000 to the local vocational college as part of its "good neighbor" program. Press reports indicated that the docking fees for the SS Tropical Paradise in Dominica were "shockingly high."
In Jamaica

June 2 - Investigators with the Jamaican National Police got a major break when they received an anonymous tip regarding funds transfers between Kingston area grocery stores and Internet bank accounts. The tip indicated that the grocery chain maintained its primary accounts at a DGA-owned offshore Internet bank. This report added to the already mounting evidence regarding suspicious transactions at daGama-controlled businesses.

In Aruba

June 18 - The head of DGA-America, Pablo daGama, met with a high ranking representative of a New York-based organized crime group and proposed that the group take advantage of the $3 billion a year turnover in the integrated financial operations of DGA-America's three Caribbean casinos in Aruba, Jamaica, and Barbados to launder money “better, faster, cheaper, and more anonymously than your current banking associates” as follows:

- The crime group would send funds to be laundered to one of the casinos either via a bank wire or through the Internet.
- If necessary, cash derived from U.S. or other operations can be brought directly to one of the casinos or, if desired, shipped without any customs checks via one of the daGamas’ shipping or freight forwarding companies.
- When the casino receives the money, a gaming account will be opened for the crime group and the funds intermingled with the casino's own money operations.
- Once in international waters the criminals follow previously scripted instructions and place specific bets on specific games at specific times. (The daGama gaming software has built in controls/trapdoors to adjust winnings and losses, if necessary by shorting legitimate gamblers, to make it appear that the criminals' win money.)
- The criminals' winnings are paid out in the form of smart cards whose value is transferred via the ship’s Internet banking to specified accounts. (In the very unlikely event that the source of these funds is questioned, the criminals will be able to produce documents/certified e-mails showing that their proceeds are the result of gambling earnings.)
- The funds will be moved anywhere the customer chooses through any number of daGama intermediaries without any risk of the financial trail being followed.

In the Bahamas

On June 5 the bank regulatory agency in the Bahamas announced that a pilot program of biometric identification would be implemented at all Bahamian banks, money remitters, and gambling venues. This program was designed to test new anti-money laundering investigation technologies under examination by the PJTF.

Biometric Identification Techniques

Biometric identification techniques allow the authentication of user identities to be implemented through a computer-controlled interface. Techniques include fingerprints, voice print analyzers and retinal scanners.

(See Tab L – Cyberspace Investigative Tools and Techniques)
In Lyon, France

June 7 – In the less than two weeks since issuing the daGama Advisory Bulletin, Interpol’s FOPAC unit received feedback from thirteen countries – all indicating daGama involvement in activities of a suspicious nature. In five of these instances criminal investigations of some kind involving the daGamas were already underway.

In San Jose, Costa Rica

August 6 - The Director of the PJTF and PJTF senior staff were briefed on a recently received Interpol FOPAC “organizational profile” of the daGamas which described a family-based money laundering enterprise with a wide range of clients, exploiting to the fullest the daGamas’ international corporate structure.

At the close of the discussion the Director called for the immediate convening of the PJTF Steering Committee for an “operational/strategic” session on what coordinated action might be taken with respect to the emergence of more sophisticated cyberspace-based financial criminal activity in the Caribbean. He expressed particular concern that activities such as the mixing of traditional and Internet gambling on cruise ships could represent a major shift in the modus operandi in financial crime and money laundering.
STEP ONE
Instructions

How to Proceed

1. You will have approximately **90 minutes** to complete your deliberations on STEP ONE.

2. You are in the role of a senior staff member of the Permanent Joint Task Force (PJTF).

3. You are in a group deliberative and drafting process finalizing a Decision Memorandum for an emergency PJTF Steering Committee meeting on a possible strategy for dealing with recent revelations confirming widespread cybercrime activities by the daGama family.

4. The Chair of your group will lead a discussion that moves through the tasking described in the Decisions to Be Made section in the column to the right.

5. The Chair will begin by asking each of the participants to very briefly give their individual perspectives - their “take” - on the key facets and overall character of the situation presented.

6. The Chair will ask one of the participants to record the group’s changes to the Draft Memo and group recommendations on specific issues.

7. **Note:** The Chair of each group will be asked to summarize the group’s deliberations and recommendations on STEP ONE (and STEP TWO) at the end of STEP TWO (see Agenda).

Decisions to Be Made

I. Issues and Options

Several members of the PJTF staff met earlier and prepared the **Draft Decision Memorandum** on the following pages. This Draft Memo provides an initial cut at what might go forward to the **PJTF Steering Committee** on a set of strategy and other issues related to the daGamas illegal activities.

Under the guidance of the Chair, the group should **expand and modify the Draft Memo as judged appropriate.** If there are issues or options beyond those presented which the group thinks should be addressed at this point in time, it should modify the Draft Memo accordingly.

2. Recommendations

   If there is a strong and unreconcilable divergence of views on some issue, the Chair will conduct a **vote on the options** still on the table and record the vote.

Keep in mind that at this point a consensus on all issues - and especially on the most difficult and divisive issues - is not necessarily expected.
STEP ONE
DRAFT DECISION MEMORANDUM

Western Hemisphere Permanent Joint Task Force

12 August 2005

MEMORANDUM FOR: THE PJTF STEERING COMMITTEE
FROM: EXECUTIVE DIRECTOR, PJTF
SUBJECT: THE DAGAMA FAMILY AND THE EVOLVING CRIMINAL MENACE TO THE CARIBBEAN VIA CYBERSPACE

BACKGROUND

The PJTF has been provided with a recently completed Interpol FOPAC "organizational profile" on the Lisbon-based daGama organization. The profile, using information supplied by twenty countries, describes a family-based enterprise which appears to be providing money laundering services for a range of criminals - exploiting to the fullest a range of emerging cyberspace technologies and the vast international corporate structure which fronts the daGama's illicit enterprise.

Preliminary evidence points in particular to the daGama's extensive use of family-owned casinos and financial institutions to move funds globally via various mechanisms. Much of this activity appears to take place through Internet and Cyberpayment transactions, greatly hindering investigative efforts.

The PJTF has also developed information that points to extensive influence peddling by the daGamases. It is worth noting that in many countries, there are daGama family members in residence who are treated as well-respected members of the upper class elite.

BASIC STRATEGY

Efforts to date by individual nations to contain the money laundering operations of the daGama family have been largely unsuccessful. In light of this situation it seems appropriate if not imperative to consider coordinated action by the PJTF to deal with the daGama family's expanding cybercrime efforts.
As a first step, it would appear advisable - in order to better guide PJTF efforts - to attempt to characterize more accurately the precise nature of the daGama problem. For example, should the daGamas' activities be characterized as random criminal activity, as organized crime, as white collar crime, or possibly even as a national security threat?

In this context we also need to decide which kind of basic law enforcement strategy might be employed against the daGamas. For example, should the PJTF undertake:

- A traditional law enforcement investigation - focus on the individuals involved or the specific underlying criminal activity;
- A linear approach - e.g., conduct the investigation from a modular perspective focusing on multiple components within the criminal organization such as supply, transportation, communications, financial, security, etc. or,
- A financial investigation - "Follow the money" approach, focusing on the financial operations associated with the underlying criminal activity.

or some kind of hybrid strategy.

In this context the following issues need to be addressed:

1. How should the daGama operation be characterized for the purpose of guiding PJTF actions?
   - A. Random criminal activity
   - B. Organized crime
   - C. White collar crime
   - D. National security threat
   - E. A combination of the above
   - F. Other

2. What overarching strategy template should be used by the PJTF to attack the daGama criminal operation?
   - A. Traditional law enforcement investigation
   - B. Linear strategy (including a Financial investigation)
   - C. Financial investigation
   - D. A Hybrid of the above
3. What should be the priority resource groups (in light of resource limitations) which the PJTF draws from for this effort (Rank order the top three or four choices)?

_____ A. Governmental law enforcement entities; e.g.,

_____ B. Multinational law enforcement entities; e.g.,

_____ C. Regulatory entities; e.g.,

_____ D. National security entities; e.g.,

_____ E. Non-governmental entities; e.g.,

_____ F. International financial institutions (e.g., the IDB, the IMF, World Bank)

_____ G.

INTERNATIONAL ISSUES

The daGama organization has cleverly exploited jurisdictional boundaries to establish a rapidly growing criminal enterprise. Furthermore, given the profits from the vast amounts of illicit funds being laundered, there is the potential for the daGamas to use their wealth to suborn the political/financial systems in the hemisphere.

In this situation there are a number of well-established legal mechanisms for international cooperation that might be employed by the PJTF. These include Mutual Legal Assistance Treaties (MLATS), Letters rogatory, Financial Intelligence Units (FIUs). These and other information sharing mechanisms have distinct positive and negative attributes which must be carefully considered by the PJTF.

1. What should be the priority mechanisms for international cooperation that the PJTF employs to pursue the daGama investigation (Rank order the top three or four choices?)

_____ A. Mutual Legal Assistance Treaties (MLATs)

_____ B. Letters Rogatory

_____ C. Interpol

_____ D. Financial Intelligence Units

_____ E. Regional Anti-Money Laundering Bodies (e.g., FATF, CFATF, CICAD Experts Group)

_____ F. Financial Information Exchange Agreements

_____ G. Use of Law Enforcement Liaisons and Attaches based in Foreign Countries

_____ I. Informal Mechanisms
J. Other

LAW ENFORCEMENT ISSUES

A number of contemporary law enforcement techniques will be affected by these emerging cyberspace and electronic commerce problems. Many of these law enforcement techniques - e.g., wiretaps, subpoenas, and the use of confidential informants - will also continue to face difficult jurisdictional problems.

This raises a question as to which traditional law enforcement techniques might prove useful in the cyberspace context, recognizing that the use of such techniques will require coordination with national authorities.

1. What traditional law enforcement techniques should the PJTF seek to employ with national authorities in support of the daGama investigations?

A. Wiretap techniques

B. Warrants, subpoenas, and other judicial orders to obtain daGama bank records

C. Confidential informants

D. Physical seizure of computers and hard drives at sites of suspected illegal cyberspace criminal activity

2. What other investigative techniques should be pursued at this time?

A. 

B. 

CYBERSPACE-RELATED INVESTIGATIVE TOOLS AND TECHNIQUES

The assessment of new cyberspace investigative tools and techniques potentially applicable to emerging problems in electronic commerce commissioned by the PJTF Advisory Board last year was recently completed.

Among the tools and techniques identified as potentially valuable for law enforcement were advanced remote system monitoring and authentication tools capable of gathering information on funds flows on the Internet. The report recommends that the PJTF undertake a modest pilot program that would test the most promising of these tools and techniques (artificial intelligence
algorithms applied to networks, biometric measures, etc.) in individual PJTF countries as a path to developing a multinational policy in this new law enforcement area.

In light of the daGama situation, the PJTF may want to accelerate the proposed program and apply some of these new tools and techniques to the daGama problem. This might be done by initially testing the techniques in a manner and in countries that would not alert the daGamas to this new effort, by testing in the countries where the daGamas are active but not initially targeting the daGama enterprises, or by applying these techniques directly to the key daGama enterprises of particular concern.

1. Should the PJTF initiate an ad hoc pilot program to apply selectively some of the cyberspace-related tools and techniques for combating cyberspace-based money laundering?

   ______ A. Yes. A pilot program should immediately be undertaken and applied as follows:

   ____ 1. Only in countries that do not have significant daGama enterprises

   ____ 2. In countries that have significant daGama enterprises but not initially targeting those enterprises.

   ____ 3. In countries that have significant daGama enterprises and targeting those enterprises.

   _____ B. No. Not at this time.
FinCEN

CFATF Exercise

Tab D

STEP TWO

4/30/98 1200

Trinidad

4-7 May 1998

RAND
STEP TWO
Instructions

How to Proceed

1. You will have a total of about two hours to complete your reading and your deliberations on STEP TWO (see Agenda).

2. You are again in the role of a senior staff member of the Permanent Joint Task Force (PJTF).

3. Your instructions are basically the same as in STEP ONE.

4. The Chair of your group will again begin the discussion by asking each participant to very briefly give their individual perspectives - their “take” - on the key facets and overall character of the situation presented.

5. **REMININDER NOTE:** The group's changes to the Draft Decision Memorandum and the group's recommendations on specific issues will again be recorded. *(Note on the Agenda that the “Presentation of STEP ONE and STEP TWO Findings” - essentially a summary and synthesis of all of the groups' STEP ONE and STEP TWO Decision Memo changes and recommendations on individual issues – will take place at 2:00 pm, immediately after lunch.)*

Decisions to Be Made

1. Issues and Options

Several members of the PJTF staff met earlier and prepared the Draft Decision Memorandum on the pages following the Situation Report.

Your instructions on expanding and modifying the Draft Memo are the same as in STEP ONE.

2. Recommendations

Your instructions on seeking consensus on recommendations on the individual issues in the Draft Memo are the same as in STEP ONE.

Again, if there is a strong divergence of views on the recommendation on some issue, vote on the options still on the table and record the vote.
Tab D

STEP TWO Situation Report

San Jose, Costa Rica

The August 12 meeting of the PJTF Steering Group produced the following outcomes on the subjects addressed:

BASIC STRATEGY:

• After extensive discussion it was agreed that the daGama family's criminal operations did not lend themselves to any one generic characterization (organized crime, national security threat, etc.) for the purpose of guiding PJTF actions.

• Similarly, no single investigative strategy seemed to lend itself best to the problems posed by the daGamas.

• In light of this situation it was decided to adopt a hybrid strategy to attack the daGama's criminal operations to include the following components:
  • Identify all significant daGama corporate holdings
  • Map out the elements of the daGama financial infrastructure
  • Determine specific daGama money laundering methods
  • Develop an evidentiary base from which nations may pursue prosecutions

INTERNATIONAL ISSUES:

• In assessing options for international cooperation and information sharing, it was recognized that there exists a range of possible approaches with various advantages and disadvantages.

• In light of this situation the Steering Group directed the PJTF to employ all possible legal mechanisms to pursue the daGama investigation - with an emphasis on:
  • Compliance with the PJTF Treaty
  • Mutual Legal Assistance Treaties (MLATS)
  • Cooperation among Financial Intelligence Units (FIUs)
  • Multinational Memoranda of Understanding (MOUs) on Information Sharing and Prosecutorial Jurisdiction
  • Multinational MOUs on Investigative Cooperation
LAW ENFORCEMENT ISSUES:

- The Steering Group directed the PJTF Operational Assistance Division (OAD) to assist appropriate national jurisdictions where required in the use of wiretaps and confidential informants, the issuance of subpoenas and warrants, and any other law enforcement techniques judged to be within the bounds of established lawful enforcement procedures.

CYBERSPACE-RELATED TOOLS AND TECHNIQUES:

- The Steering Group directed the PJTF to initiate a modest pilot test program for cyberspace investigative tools and techniques in a small number of PJTF countries – the countries to be chosen by the Director of the PJTF after consultation with respective governments. If possible, some of the countries selected should be among those where daGama activities of particular concern are taking place.

San Jose, Costa Rica

Late August - In collaboration with the governments of Dominica, Trinidad and Tobago, the Cayman Islands, and the United Kingdom, the PJTF Operational Assistance Division initiated a multi-pronged investigation of the daGama family. Overall responsibility for coordinating the various operations was assigned to the Director of the Operational Assistance Division.

The priority targets of the multinational operation were:

- The daGama cruise ship SS Tropical Paradise currently in Dominica
- The daGama Internet operations in Trinidad and Tobago
- The Cayman Islands branch of the daGama-owned CDL Bank (headquartered in Lisbon)

Each of these targets was judged to play a key role in the daGama money laundering operation.

For its part, PJTF headquarters agreed to coordinate with member governments to:

- Provide financial investigators to work on-site with local authorities
- Make available technical assistance to initiate:
  - Electronic surveillance
  - Undercover or “controlled delivery” operations
- Provide banking auditors to work on-site with local authorities
- Create and maintain a central database on the daGama enterprise
- Provide international law specialists to participate in the development of a multi-national prosecution strategy

By mid-September major efforts were underway against the three priority daGama targets cited above.
San Jose, Costa Rica

October 20 - The Director of the Operational Assistance Division (OAD) briefed the PJTF Steering Committee on the evidence that had been gathered through the operation in Dominica targeting the daGama-owned SS Tropical Paradise. A Dominican court had issued an order that had allowed investigators to conduct a computer monitoring operation involving an intrusion into the ship's database management system.

The briefing detailed the history and character of the information that had been gained to date regarding the flow of money through the ship. Based on this information, PJTF analysts had been able to produce a rough but increasingly disturbing picture of a highly complex daGama financial infrastructure.

London, England

October 25 - The head of the Metropolitan Police Department's Company Fraud Squad briefed the Director of the PJTF-OAD on information that Scotland Yard had gleaned through a “controlled delivery” operation involving two highly-placed employees of the daGama-owned IST Securities, an Internet-based trading company. The operation had successfully “turned” the two trusted company employees who faced prosecution and potentially long jail terms had they chosen not to cooperate.

For the past two months, acting on instructions from their police “handlers,” the two cooperating defendants had continued to operate a long-running layering scheme on behalf of the daGama family:

- On an almost daily basis, in-bound funds transfers came from daGama banks in the Caymans and Lisbon.
- In some cases, the transfers occurred through the traditional wire systems; more often, the money came in via Internet-based e-cash transmissions.
- The securities transactions were always conducted on behalf of offshore holding companies, none of which appeared to have direct daGama family links.
- Investigators believe that the holding company accounts may have been the final transfer point prior to the laundered funds being sent back to the daGama client.

The Company Fraud Squad had documented more than $47 million in suspect transactions and believed that adequate evidence existed to move toward the indictment of several individuals involved in the activities, but so far had been unable to develop a case for action against any members of the daGama family. In this situation, Scotland Yard was interested in whether the PJTF could provide data on the branch of the daGama-owned CDL Bank in the Cayman Islands.

Roseau, Dominica

December 23 - Based on the steady flow of data from the computer intrusion on the SS Tropical Paradise, PJTF analysts reported to a meeting of member country bank regulators that they had now pieced together a detailed picture of the daGama financial infrastructure - which one regulatory official characterized as “an operation with the capability to compete with major international financial institutions.”
Within this construct, the PJTF analysts described two specific activities which they judged to be potentially indicative of a money laundering operation:

- Each Saturday, the computer logs show a “Cash Received” category with multiple entries generally between $10 and 25 million dollars - an amount far exceeding the daily entries associated with the legitimate gambling activity. PJTF analysts speculate that this weekly cash influx may be criminally based.

- At four-hour intervals, 24 hours a day, seven days a week, electronic funds transfers are made from the SS Tropical Paradise. The transfers are always sent to three banks, all owned by daGama holding companies.

While the latter type of transfer procedure is not in and of itself unusual, the aggregate dollar amount involved is several times that associated with a casino operation of the Tropical Paradise’s size - and commensurate with the aggregate amounts that come in on Saturdays.

**Port of Spain, Trinidad**

December 28 - The Director of the Trinidad Strategic Services Agency informed the PJTF that their previously highly successful intercept operation had been unexpectedly “shut down” with “no hope of being reestablished” due to a new highly encrypted communications link being used in the daGama operations in Port of Spain.

He noted, however, that a final intercept recorded on December 19 included mention of “digital keys” and a discussion of a new Internet-based funds transfer system to “service the North Points Resort,” a daGama enterprise that had just opened on Trinidad’s west coast. The resort is believed to have been funded through daGama-laundered Colombian drug money.

The new funds transfer system being installed was noted to be a product of SellNet Solutions, a daGama owned software company based in Singapore.

**San Jose, Costa Rica**

January 7 - Investigators in Dominica informed the Director of the PJTF-OAD, via an encrypted satellite telephone, that after five months of successful intercepts, the computer-based surveillance operation of the SS Tropical Paradise had been compromised. A new encryption package had been activated within the ship’s data management system. Within hours PJTF cryptology experts had judged the prospect of breaking the new encryption package as “highly unlikely” in the near term.

**Port of Spain, Trinidad**

January 10 - Based on the previous intercept activity and on suspicious activity reports filed by a local Trinidad bank, a task force established to investigate the financial operations of the North Points Resort moved quickly to subpoena the resort’s bank records. An analysis of the records showed that the North Points Resort accounts were “through points” with frequent e-cash transmissions in and out.
Unfortunately, given the “one way anonymity” characteristic of the e-cash payment instruments, the investigators were unable to determine either the sources or the recipients of the funds. They were, however, able to determine that some of the transfers were conducted via a new local Internet service provider, TriniNET, and an Antigua-based data server, both of which appear to be owned by a daGama parent company.

Technicians also had limited success dealing with the encrypted e-mail and communications packages. However, they were able to decode two e-mail messages that showed that more than $250 million dollars had been transferred through the Antigua-based server to the daGama-owned CDL Bank in Lisbon.

**Cayman Islands**

January 14 - The Cayman Islands Financial Intelligence Unit (FIU) attempted to investigate an informant’s claim that the Caymans branch of the daGama-owned CDL Bank was engaging in money laundering. The allegation stated that the bank was facilitating the transfer of tainted digital coins and stored value smart cards, and disguising the origins of the funds as gambling proceeds.

The FIU subpoenaed and obtained the bank’s records, including computer software and hard drives, but was unable to interpret the highly encrypted data. However, PJTF technical experts were able to decipher a significant portion of the e-mail records which detailed links from the bank to a South American drug cartel and the Trade Winds gaming operations on board the SS Tropical Paradise.

**San Jose, Costa Rica**

January 16 - The head of the PJTF – Operational Assistance Division (OAD) briefed the PJTF Executive Director on the “gold mine of data” from the Caymans’ CDL Bank’s files. He recommended that the PJTF Executive Director and the Chairman of the PJTF Steering Committee approach the Cayman Islands government with a demarche to close down this offshore facility and begin a criminal prosecution against specific members of the daGama family.

Data from the copied CDL Bank computer discs had revealed that offshore deposits into the bank were generated by money laundering activities by bank customers located in the United States, the United Kingdom, and Canada – represented on the Caymans’ CDL Bank books as the proceeds of Internet gambling activities on Trade Wind’s cruise ship casinos.

In order to conceal these ostensible “high roller” winnings from national taxation authorities, Trade Winds “preferred customers” routed these funds through “placeholder” accounts in the Caymans’ CDL Bank using a highly encrypted data transfer application issued to them by the Lisbon office of the CDL Bank.
The encryption application - while in compliance with U.S., UK., and Canadian encryption standards - contained an undocumented data concealment (high level-encryption) capability which was embedded in overt message traffic generated by these data streams.

The decrypted data revealed that when funds transfers from a personal computer of one of the ostensible "high rollers" were sent to the Caymans' CDL Bank, a highly encrypted "virtual private network" (VPN) would come into operation thereby removing such traffic from the purview of normal traffic analyses techniques. This permitted Caymans' CDL Bank to operate two sets of books - one generated by the international digital signature infrastructure that created records of legitimate funds transfers over the Internet and the other a set of books recording secret transfers of income into confidential accounts maintained on a protected server at the CDL Bank branch office in the Caymans.

![Diagram of CDL Bank Funds Concealment]

**Figure 1. CDL Bank Funds Concealment**

As shown in Figure 1 above, the process operated as follows:

1. Internet Gamblers receive a gaming software application from the Internet Casino operators.
2. The gaming application decrypts an encrypted transfer of value (remittances) from the casino.
3. The application then reads an encrypted message header and covertly transfer funds to an offshore account.
4. The Internet casino maintains records of an understated value transfer; the Secure Server at the Bank of El Porto holds comprehensive records on the size and timing of customer deposits.
San Jose, Costa Rica

January 30, 2006 - In a videoconference with the PJTF Steering Committee, the Executive Director described the key components of the highly sophisticated daGama money laundering operation - essentially a "closed loop" of Internet service providers, Internet banks, and casinos used to launder funds on behalf of various clients - and many of the key players involved. The daGamas have creatively integrated this cyberspace money laundering with traditional banking, land-based resorts and casinos, financial management companies, and a host of other initiatives to greatly complicate the flow of funds within the corporate empire.

The meeting concluded with a tentative agreement among the Steering Committee to begin focusing and coordinating their efforts toward the development of a prosecution strategy against the daGamas.

The Day After...

Cayman Islands

February 8, 2006 - While the Caymans’ FIU had collected a significant amount of anecdotal evidence (especially from the two cooperating informants in London) linking the Caymans’ CDL Bank to a suspected money laundering operation involving daGama cruise ship operations, they realized that they lacked sufficient records needed to bring a successful prosecution.

In an attempt to expand the scope of the case, on February 8 the head of the Cayman FIU approached the Inspector of Financial Services/Caymans Financial Services Supervision Department to discuss the possible availability of regulatory banking records and the legal application of such records in a criminal investigation.

The Inspector of Financial Services ruled that the facts warranted an exception to the confidentiality provisions normally associated with the banking records. He noted, however, that many of the bank’s activities appear to have occurred in other jurisdictions, and as such, access to certain records would require specific authorization of the Governor in Council and the High Court - and promised to expedite such requests.

Roseau, Dominica

February 9 - The SS Tropical Paradise returned to dockside after a three week cruise of the Caribbean which included stops in Grenada, Martinique, the British Virgin Islands, Puerto Rico, and Jamaica.
Cayman Islands

February 10 - At noon local time access to the Caymans' CDL Bank's records was granted to the Caymans FIU. An hour later, in a dramatic action seen on local television, the hard drives and other bank equipment were seized and several bank officials arrested.

Cayman Islands

February 20 - In a “profoundly disappointing” after action report, Cayman authorities described how the daGama organization had moved quickly, and “probably on the basis of a tip,” to route suspect funds out of the Caymans' CDL Bank via dedicated daGama banking channels.

The bank's records showed that money from entities appearing to be fully legitimate remained on deposit, and new funds, also seemingly legitimate, had suddenly appeared in the bank. The Cayman authorities concluded that the daGamas had played a successful “electronic shell game,” shifting funds around in cyberspace.

Further, Cayman auditors and inspectors suspected that the bank used a special software program which generated backup documentation for the new account activity although this had not been confirmed. They suspected that somehow a second set of “digital books” had been created; however, given the unique operating characteristics of an Internet bank, they were left with few clues as to the location of these records.

The Cayman authorities concluded in their report that the investigation was left with little useful evidence and that they could not recommend criminal or civil proceedings against the Caymans' CDL Bank branch.

Roseau, Dominica

March 4 - Data from the PJTF/Dominican operation led prosecutors to indict 27 employees of the SS Tropical Paradise, as well as five executives at Trade Winds SA, the ship's parent company.

The Dominican indictments were drawn and based largely upon evidence collected through the computer monitoring operation.

In Lisbon

March 8 - A spokesperson for the daGama parent corporation in Lisbon denounced the “wild rumors” surrounding the SS Tropical Paradise and the Trade Winds SA and claimed that these daGama enterprises would be proven innocent of the Dominica charges. She further noted that Trade Winds SA had been “unfairly tarred by ruthless commercial competitors which included several American and European cruise ship and gaming interests which operated out of Florida.”
The U.S. and British Ambassadors to Portugal sent parallel messages to their capitals noting that the daGama family would likely now go into a "defensive crouch" and launch an all-out media blitz to defend itself from negative publicity flowing from the Dominica indictments.

**Port of Spain, Trinidad**

March 9 - Using information obtained through its *North Points Resort* informant, the Trinidad Task Force was given a search warrant for the homes of four resort executives and the financial management office at the resort's casino with the objective of "uncovering the financial infrastructure of a probable money laundering scheme."

Authorities seized four network computers but quickly discovered that the computers were little more than "shells" used to transmit and receive e-cash between off-shore Internet servers.

**Port of Spain, Trinidad**

March 11 - In a briefing to Trinidad's senior law enforcement officers, the Task Force's forensic computer investigation specialist surmised that the computers found at the casino were used strictly as "transmission devices" in which money leaves the computer for a destination in cyberspace where it is stored - with no records maintained on-site. In theory, the records for this system could be at "any number of different servers in a dozen different countries." Similarly, money coming back into the casino would enter the computer and be quickly "downloaded to a device such as a smart card, or transmitted to another location in cyberspace" via the Internet.

Given this finding and lacking financial records to support the anecdotal evidence previously collected, the Task Force found itself unable to pursue a prosecution at this time.

**Roseau, Dominica**

April 6 - In spite of what had appeared to be a very strong case, the Dominica prosecution was put in jeopardy when defense attorneys representing the *Trade Winds* executives filed a motion with the Dominica court calling for dismissal of all criminal charges.

Their motion argued that Dominica lacked jurisdiction in the matter since the activity presented in the criminal complaint occurred aboard the *SS Tropical Paradise*, a vessel registered to the sovereign nation of Liberia. They argued further that the vessel spent approximately 75% of its time outside of Dominican territorial waters and many of the specific charges pertain to activities that occurred while the ship was at sea.
Roseau, Dominica

April 7 - In a tersely worded response, the Dominican Court ruled that the *SS Tropical Paradise*, when in Dominica, was subject to Dominican law, regardless of its Liberian registration. However, regarding the matter of activities which occur while the ship is at sea, the Court found that: “The Government may claim jurisdiction only over violations of law which occur within its geographic boundaries.”

Based upon this ruling, many of the specific counts in the indictments had to be dropped by the prosecution. The Dominican prosecutors stated, however, that they continued to be confident that many of the defendants would be convicted based upon activities which occurred while the *SS Tropical Paradise* was in port.

Roseau, Dominica

April 9 - The *Trade Winds* defense team filed another motion, this time challenging the legality of the Governments surveillance operation against the *SS Tropical Paradise*. In response, the prosecution argued that the computer monitoring operation was lawfully initiated following the issuance of subpoenas by the proper Judicial authority, in accordance with Dominica’s criminal code.

The case was held up for several weeks as the Dominican judge considered the matter - ultimately deciding to forward the matter to the High Court for resolution.

Roseau, Dominica

May 5 - In a split decision, the High Court found in favor of the defense, ruling that Dominica’s Electronic Surveillance Law was written specifically, and exclusively, for the purpose of authorizing the intercept of telephone-based transmissions, not as a catch-all authorization for electronic media.

The Court went on to note that the unique operational characteristics of computers, particularly those linked via networks, are significantly different than the characteristics and capabilities of a telephone, and therefore, the standards for Government access to these systems must be examined as independent matters.

The court ruling left the Dominica prosecution with an extremely fragmented case. Although many of the team members felt they could still successfully move forward against half of the original defendants, on May 6 the lead Dominican attorney reluctantly requested a dismissal of all charges.

San Jose, Costa Rica

May 6 - The Director of the PJTF asked his deputies to prepare a memorandum to the PJTF Steering Committee outlining possible new courses of action in terms of PJTF support to the three key daGamas investigations in the light of recent events in those investigations.
Western Hemisphere Permanent Joint Task Force

May 8, 2006

MEMORANDUM FOR: PJTF STEERING COMMITTEE
FROM: EXECUTIVE DIRECTOR, PJTF
SUBJECT: PJTF SUPPORT TO THE DAGAMA INVESTIGATION

BACKGROUND

As you know, the PJTF has been providing assistance to Dominica, Trinidad & Tobago, and the Cayman Islands with regard to the following efforts:

1. The Dominican investigation and prosecution of *Trade Winds SA*, in connection with money laundering activities on board the cruise ship, *SS Tropical Paradise*.
2. The Task Force investigation in Trinidad, targeting the daGama drug money laundering activities at the North Points Resort.
3. The Cayman Islands investigation of money laundering activities through the daGama-owned *CDL Bank*.

All three national efforts can be judged as a mixture of: (1) important initial intelligence successes leading to (2) important discoveries about the daGama's operations, but in the end in each case (3) a failure to achieve successful prosecution.

In considering how to proceed in this situation, for the purpose of clarity and analysis we have classified two different types of regulatory, law enforcement, and prosecutorial failures:

- A “Type A” failure in which the national effort to investigate and prosecute a criminal breaks down because of a lack of adequate regulations and laws.
- A “Type B” failure in which the targeted criminal enterprise is able to take advantage of the new features of Cyberspace to deny the acquisition of useable evidence and/or otherwise avoid prosecution.

Each of the national operations is discussed in further detail below.
THE THREE NATIONAL OPERATIONS

The Dominican Prosecution of the SS Tropical Paradise as a Type A Failure

The Dominican effort to penetrate the data systems of the SS Tropical Paradise with PJTF assistance was operationally and technically successful for a period of time. Invaluable data was gathered to build a picture of how the daGama money laundering enterprise takes advantage of the unique features of Internet gambling capabilities. Unfortunately, Dominican law has not been fully developed to take into account the new technological modes of police surveillance. Thus, an apparently successful prosecution strategy was thwarted by the skillful exploitation of a legal loophole by the defense lawyers of Trade Winds SA.

The Trinidad and Tobago Investigation of the North Points Resort as a Type B Failure

Based on information obtained by local law enforcement, investigators in Trinidad attempted to seize evidence in a raid on the North Point Resort. However, the facility turned out to be simply an Internet service provider that acted as a waypoint for massive data flows with all incriminating data apparently stored at sites outside of the Caribbean. No computer or written records of consequence were found and prosecution of the North Point Resort was not pursued.

The Cayman Island Investigation of the CDL Bank as Partial Type A and B Failures

The Cayman Islands Financial Intelligence Unit (FIU) with assistance from the PJTF and Scotland Yard developed strong indications of money laundering activity at the Caymans branch of the daGama’s CDL Bank. The investigators attempted to broaden their case through an audit of the suspect bank’s records but during the course of the more than eighteen hours required to gain such authority, the bank was able to play a successful “electronic shell game” by shifting funds via cyberspace. Further, Cayman auditors and inspectors had evidence that the bank used a special software program that generated backup documentation for the new account activity that was legitimate. This demonstrated the ready capacity of a financial institution to keep more than one set of books on cyberspace financial transactions.

The latter incident in particular highlights the need for more timely legal and law enforcement response options to deal with a very agile financial crime target.

NEXT STEPS

The above-described incidents point to the major challenges to law enforcement, judicial authorities, and regulators posed by the arrival of very sophisticated transnational criminal organizations which operate through cyberspace. It is clear that the PJTF and like-minded organizations will need to step back and analyze this developing situation in depth in pursuit of a more effective long-term strategy for dealing with these new kinds of problems.

Furthermore, aggressive law enforcement action - and cooperation on the part of PJTF members, even if not wholly successful against the daGamases - may serve to give notice to would-be cyberspace money launderers that the PJTF countries are determined to aggressively pursue financial crime taking place in cyberspace.
NEW INITIATIVES IN ONGOING INVESTIGATIONS

The upcoming PJTF Steering Committee meeting provides an opportunity for high-level consideration of further PJTF-coordinated action against the daGamas. In particular there may be attractive intelligence gathering opportunities in other PJTF nations where the daGamas operate businesses (see wall charts).

In this context, a renewed look at our strategy in each of the national efforts is called for:

1. *In the Dominica Investigation:* What new initiatives might be undertaken in Dominica or in other PJTF countries relating to the daGama investigation?
   
   •  
   
   •  
   
   •  

2. *In the Trinidad Investigation:* What new initiatives might be undertaken in Trinidad or in other PJTF countries relating to the daGama investigation?

   •  
   
   •  
   
   •  

3. *In the Cayman Islands Investigation:* What new initiatives might be undertaken in the Caymans or in other PJTF countries relating to the daGama investigation?

   •  
   
   •  
   
   •  
PILOT PROGRAMS EXPLOITING EMERGING CYBERSPACE INVESTIGATIVE TOOLS AND TECHNIQUES

Another consideration at this point in time is the possibility of exploiting promising technologies from the modest pilot programs that we have had underway on various cyberspace investigative tools and techniques. Of particular importance are the following authentication, data capture, and detection technologies:

- Network-born Tracking Devices: Software or hardware systems designed to trace data as it transits a packet-switched network.

- Digital Links: A label attached to email, data, or electronic value within a network that authenticates the identity or system access rights of particular individuals or entities.

- Artificial Intelligence Programs: Computers and software programs designed to mimic human reasoning and learning processes through the discovery of heuristics (rules) and algorithms that are then used to analyze a collection of data.

- Biometric Devices: Hardware and software systems that authenticate the identities of human beings through the capture of unique data characterizing physical features of the human body. Examples include computer-coded images of a person's finger, palm, or face, a laser-scan of an individual's retina, and a voiceprint record.

Each of these technologies represents a near-term possibility for use—as a minimum—as a means for identifying persons over the Internet. A criteria for inclusion in this list is that each product area either have commercial products already available, or that systems be in the latter stages of an engineering development process.

The need and opportunity presented by the daGama situation may argue for immediate application of some of these data gathering techniques in ongoing PJTF anti-money laundering efforts.

An important consideration in most of the possibilities presented below is that unprecedented national cooperation will likely be required—meaning that we will be asking nations to show creativity in reconciling their existing legal and regulatory codes to permit proposed actions.

1. **Network-Born Tracking Devices:** Should the PJTF initiate and coordinate the use of network-born tracking devices in the daGama investigations—and if so where?

   ____ A. Yes. Initiate the use of these devices as follows:

   - ____________________________

   - ____________________________

   ____ B. No. Efforts of this nature should be handled by individual nations.

   ____ C. No. Action of this nature is inappropriate at this time.
2. Digital “Links” Connecting Financial Bits and Owners: Should the PJTF initiate and coordinate the capture of data from digital “links” (digital signatures) which connect financial bits and their owners in the daGama investigations - and if so where?

___ A. Yes. Initiate the use of these devices as follows:
   
   • 
   
   • 
   
   •

___ B. No. Efforts of this nature should be handled by individual nations.

___ C. No. Action of this nature is inappropriate at this time.

3. Artificial Intelligence Programs for Internet-Based Financial Transactions: Should the PJTF initiate and coordinate the use of artificial intelligence programs for capturing data from Internet-based financial transactions in the daGama investigations - and if so where (e.g., in specific gambling venues in specific countries)?

___ A. Yes. Initiate the use of these devices as follows:
   
   • 
   
   • 
   
   •

___ B. No. Efforts of this nature should be handled by individual nations.

___ C. No. Action of this nature is inappropriate at this time.

4. Biometric Identification Devices: Should the PJTF initiate and coordinate the capture of data from biometric identification devices in the daGama investigations - and if so where (e.g., in specific gambling venues in specific countries)?

___ A. Yes. Initiate the use of these devices as follows:
   
   • 
   
   • 
   
   •

___ B. No. Efforts of this nature should be handled by individual nations.

___ C. No. Action of this nature is inappropriate at this time.
TAB E
STEP THREE INSTRUCTIONS

How to Proceed

1. You will have a total of two and one-half hours to complete your reading and deliberations on STEP THREE.

2. In this step you are now back in the present.

3. Your task is to evaluate and rank order a set of alternative issue areas for addressing cyberspace financial crime in terms of their priority for further action and policy development.

4. In evaluating some of these issue areas you may wish to refer to the material found in Tab L of your briefing book on “Cyberspace Investigative Tools and Techniques.”

5. The chair of each will again be asked to summarize the group’s deliberations and recommendations in the plenary session that takes place after the completion of STEP THREE.
STEP THREE

Introduction

With respect to the emerging Cyberpayment, Internet banking, and Internet gambling components of electronic commerce, the significant money laundering-related policy issues may be divided into four categories: (1) Due Diligence; (2) Oversight and Supervision; (3) Law Enforcement; and (4) Legal.

Due Diligence

Due Diligence refers to the measures taken by financial service providers to ensure the soundness of the institution, as well as the integrity of those conducting business with the institution. Under the broad heading of Due Diligence, four sub-categories may be identified:

Identification: When establishing customer relationships, financial service providers take steps to ensure that transactions are conducted by the lawful individuals known to the institution. In the cyberspace environment, however, authenticating a transactor's identity may present new challenges to the financial institution.

Know Your Customer: (KYC) plays a central role in existing governmental and multinational anti-money laundering programs. It is critical that financial institutions monitor/examine customer activity to ensure that it is commensurate with what is expected of that customer or similar customers. However, in the world of electronic commerce, an environment with little or no physical interaction between the financial service provider and the customer, existing KYC mechanisms may have to be revised/expanded to remain effective.

Record Keeping: There exist today, in almost all nations, standards for filing and maintenance of records pertaining to all financial transactions conducted through regulated institutions. In the realm of electronic commerce, however, some types of transactions may fall outside the scope of existing Record Keeping regulations.

Suspicious Activity Reporting: (SAR) has been recognized in many international fora as an effective anti-money laundering tool. SAR programs of varied character have been developed, each taking into account regional differences and practices. The same flexibility will be necessary when establishing SAR criteria for Cyberspace. Are activities which are considered "suspicious" and therefore reportable in the brick and mortar banking world, the same, or the only, activities which should cause concern, if observed in the Internet banking context?
Oversight and Supervision

Oversight and Supervision refers to the regulatory policy and enforcement responsibilities of governmental authorities with regard to financial service providers. This broad category may be broken into components, the first of which is Licensing. Although most nations have established regulations pertaining to banks and other financial service providers, there may be potentially unique licensing requirements associated with institutions which operate in cyberspace.

Also within the scope of Oversight and Supervision comes the issue of Payment Instrument Functionality. As electronic commerce emerges, some nations have taken regulatory and legislative measures to mandate the operating characteristics of Cyberpayment, Internet banking, and Internet gambling products. However, other nations have chosen to “wait and see” how the industries develop.

Examination also plays a key role in the Oversight and Supervision process and also presents potentially significant challenges in the cyberspace context. The rules and techniques for auditing financial activity on the Internet are still being developed. The issue of examination becomes more complicated when raised in the context of activities that may occur in or impact multiple jurisdictions.

Law Enforcement

Governmental authorities have developed progressively more effective mechanisms and techniques for the investigation of money laundering and other kinds of financial crime. However, these investigative techniques were created within the context and limitations of the traditional payment system. With the advent of electronic commerce, these proven law enforcement programs must be continually assessed to determine their effectiveness.

Within this context, technology may present both challenges and opportunities for Law Enforcement. The Cyberpayments, Internet banking, and Internet gambling components of electronic commerce, if left unchecked, could be vulnerable to exploitation for criminal purposes and may compel authorities to consider and/or develop new investigative techniques. At the same time, however, the new technologies, by virtue of their operating characteristics, may also facilitate innovative cyberspace-based investigative tools by providing new and automated means to collect relevant information.

Legal

There are many Legal issues raised by the emergence of electronic commerce. Some countries may lack the statutory base from which to investigate and prosecute cyberspace-based crime. They may lack the rules of evidence to utilize certain types of information which are unique to cyberspace. In addressing this concern, some nations attempt to apply or modify existing law to fit the cyberspace environment. In some instances, new laws are being enacted to focus specifically on cyberspace-based criminal activity.
Even more challenging international legal problems may appear due to the "borderless" nature of cyberspace. Even if appropriate cyberlaws exist in a particular country, could or should they apply in instances where some of the activity may have occurred in multiple jurisdictions? Complicated issues such as this must be addressed in international fora to ensure some degree of compatibility among jurisdictions.

RANK ORDERING OF ISSUES

Under the direction of the chair of your group, rank order the issue areas or issues on the following pages in terms of their priority for action and further policy development in two steps:

1. First, within the four major issue categories (Due Diligence, Oversight and Supervision, Law Enforcement, and Legal Issues).

2. Second, across all four major categories.

In the first step, attempt to reach consensus on the top three or four issues in each category.

In the second step, attempt to reach consensus on the top five or six issues overall.
### Due Diligence Issues

<table>
<thead>
<tr>
<th>Within Due Diligence</th>
<th>Issues</th>
<th>Across All Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Know Your Customer Issues</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. Defining unique identity authentication requirements for certain classes of cyberspace financial products and services.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. Developing international norms for cyberspace &quot;Know Your Customer&quot; measures and procedures.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>c. Monitoring and enforcement infrastructures for coordinating cyberspace &quot;Know Your Customer&quot; rules and regulations.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>2. Identification Issues</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. Employing biometric techniques and identification requirements for Internet gambling, Internet banking, and Cyberpayment applications.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. Employing digital signatures and encryption to establish a safe secure infrastructure for the authentication of digital transmissions in Internet gambling, Internet banking, and Cyberpayment applications.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>3. Record Keeping</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. Coordinating of record keeping requirements in electronic commerce applications.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. Sharing of information in cyberspace financial crime investigations.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>c. Providing incentives for good behavior by Internet banking, Internet gambling, and Cyberpayment financial services providers.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>d. Monitoring of network data in real time to detect cyberspace financial crime.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>e. Establishing an information system to enhance the investigation of cyberspace financial crime.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>4. Suspicious Activity Reporting</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Oversight and Supervision

<table>
<thead>
<tr>
<th>Within Oversight &amp; Supervision</th>
<th>Issues</th>
<th>Across All Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Licensing</td>
<td>a. Establishing rules governing permissible operators of Internet gambling establishments</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. Establishing rules governing permissible operators of Cyberpayment systems</td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. Establishing rules governing permissible operators of Internet banks</td>
<td></td>
</tr>
<tr>
<td>2. On-site Inspection</td>
<td>a. Collaborative information gathering at Internet-banks</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. Techniques for on-site inspection in cyberspace</td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. Remote surveillance of Internet financial services providers</td>
<td></td>
</tr>
<tr>
<td>3. Examination</td>
<td>a. Role of mandatory filings in international oversight activities</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. Extra-territorial investigations of Off-shore Internet banks</td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. Extra-territorial investigations of Off-shore Internet gambling establishments</td>
<td></td>
</tr>
<tr>
<td></td>
<td>d. Oversight and jurisdiction questions concerning international cyberspace financial services operations.</td>
<td></td>
</tr>
<tr>
<td>4. Transaction Thresholds</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>a.</td>
<td>Restrictions on the functionality of Cyberpayment instruments</td>
<td></td>
</tr>
<tr>
<td>b.</td>
<td>Denomination limits on smart cards</td>
<td></td>
</tr>
<tr>
<td>c.</td>
<td>Currency exchange limits for Internet banks</td>
<td></td>
</tr>
<tr>
<td>d.</td>
<td>Currency exchange limits and reporting requirements for Internet gambling establishments</td>
<td></td>
</tr>
<tr>
<td>e.</td>
<td>Development of international norms on record-keeping threshold triggers for cyberspace funds transfers and transactions</td>
<td></td>
</tr>
</tbody>
</table>
### Law Enforcement Issues

<table>
<thead>
<tr>
<th>Within Law Enforcement</th>
<th>Issues</th>
<th>Across All Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>a. Determining the relevance of wiretaps and other means of electronic surveillance.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. Employing tools and techniques for intercepting communications over computer networks.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. Determining the utility of undercover operations in investigating cyberspace financial crime.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>d. Determining the role of confidential informants in investigating cyberspace financial crime.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e. Determining the role of mandatory filings in combating cyberspace financial crime.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>f. Establishing privacy and law enforcement access to cyberspace financial records.</td>
<td></td>
</tr>
</tbody>
</table>

### Legal Issues

<table>
<thead>
<tr>
<th>Within Legal Issues</th>
<th>Issues</th>
<th>Across All Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>a. Establishing comparable laws and regulations governing cyberspace financial crime.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. Seeking common definitions of “legitimate” and “illegitimate” cyberspace financial activity.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. Determining the admissibility of computer records in international cybercrime investigations.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>d. Determining the role and utility of Mutual Legal Assistance Treaties (MLATs) and Letters Rogatory in combating cyberspace crime.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e. Exploring extraterritorial issues and the determination of appropriate jurisdictions in the investigation and prosecution of cyberspace crime.</td>
<td></td>
</tr>
</tbody>
</table>

109
CARIBBEAN FINANCIAL ACTION TASK FORCE
&
COMMONWEALTH SECRETARIAT

Workshop on
Money Laundering Through
Emerging Cyberspace Technologies

Conclusions and Recommendations

Trinidad Hilton International Hotel
Port of Spain, 4 - 7 May 1998
CONCLUSIONS AND RECOMMENDATIONS

BACKGROUND

1. In August 1997, Law Officers and Ministers of Legal Affairs of Small Commonwealth Jurisdictions met in Barbados under the aegis of the Commonwealth Secretariat and, *inter alia*, noted that computer related, high tech and Internet crime demanded an international response.

2. They were concerned that Cyberpayment instruments used in Internet activities have the potential to add new dimensions to the problems of money laundering. In this regard, Internet gambling was of particular concern to jurisdictions.

3. In recognising the inevitability of a multilateral approach to licensing and regulation of Internet activities, the Law Officers and Ministers called upon Commonwealth Governments to seek to influence the development of a multilateral response.

4. Similarly, when the Council of Ministers of the CFATF met in Bridgetown in October 1997 they endorsed the work plan of the CFATF for the year 1997/98 and authorised that organisation to develop a programme of activities aimed at sensitising regional governments to the possibilities of money laundering through emerging Cyberspace technologies.

5. In pursuance of the decisions of those two meetings the CFATF and the Commonwealth Secretariats (hereafter "the Secretariats") organised a workshop in the region to discuss "Money Laundering through Emerging Cyberspace Technology". The Workshop was held in Port of Spain, Trinidad, May 4-7 1998.

METHODOLOGY

6. Participants at the workshop were presented with a hypothetical situation set in the year 2005 and involving a well established merchant family with extensive operations in the Caribbean, the Americas and Europe operating through a network of companies some of which conducted legitimate business and the others of which engaged in money laundering activities. The companies used the Internet and Cyberspace extensively for carrying out their operations.

7. The workshop considered the ramifications of the simulated scenario under the following broad headings:

a. Due diligence issues;
b. Oversight and supervision;
c. Law Enforcement; and
d. Legal issues.
CONCLUSIONS

8. The workshop requested the Secretariats to advise governments that:

a. there is a need to encourage economic growth in Caribbean countries through appropriate use of the Internet and information technology generally. However, governments must be aware of the potential for criminal abuse of computers, computer networks, and cyberpayment mechanisms.

b. there are many and varied difficulties inherent in monitoring and regulating Internet activities;

c. governments should pay particular attention to Revised FATF Recommendation 13 which urges that special attention be given to money laundering threats posed in new or developing technologies and that appropriate measures be taken to prevent their use in money laundering schemes;

d. effective countermeasures addressing the criminal use and abuse of computers, computer networks, and cyberpayment mechanisms require substantial international cooperation; and

e. notwithstanding the need for such international cooperation, each government should take steps to develop, in cooperation with the private sector, adequate national responses. In particular, governments should ensure that legislation provides criminal sanctions and civil remedies for the misuse of computers and computer networks and provides for the collection, preservation and admissibility, in proceedings, of electronic evidence obtained from computers and computer networks.

9. The Workshop recommended endorsement of, and support for, the recommendations of the Meeting of Law Officers and Ministers of Legal Affairs of Small Commonwealth Jurisdictions.

10. The Secretariats were requested by the Workshop to consult with member governments to develop proposals to tackle crime through emerging Cyberspace technologies.

11. The Secretariats were asked to study and evaluate proposals by private sector Internet Service Providers and the electronic financial services industry for self regulation of the industry and regulation by governments and to report to governments on their findings.

12. The Secretariats were requested to initiate collaboration with other international organisations with a view to developing an appropriate multilateral response to the challenges posed by potential abuse of the Internet and Cyberspace through emerging technologies. Commonwealth jurisdictions recalled the work commenced in 1990 by Law Ministers on the development of a Scheme relating to Mutual Assistance Between
Business Regulatory Agencies and asked that Commonwealth Law Ministers be advised of their view that such a scheme had particular relevance to supervision and regulation of traditional and emerging financial activities. Accordingly they recommended that Ministers revisit this proposal and consider how it might be furthered to assist in the field of Cyberspace regulation.

13. The Workshop advised the Secretariats that their research and development work should take into account the views of the Workshop on the following issues:

a. In the context of oversight and supervision and due diligence:
   - the particular relevance of enhancing “know your customer” procedures to incorporate technology for the authentication of identity in Cyberspace;
   - the usefulness of digital signatures and encryption techniques;
   - the need to develop information systems to allow for the maintenance of records and appropriate monitoring of network activity, and which will facilitate the acknowledged need for enhanced international sharing of information;
   - the continued relevance of suspicious activity reporting;
   - the need to adapt licensing procedures to cyber technology; and
   - the need to develop appropriate supervisory regimes adapted to Cyberspace.

b. In the context of law enforcement:
   - subject to proper judicial oversight and appropriate protection of the right to privacy, the relevance of the various techniques, both existing and future, which permit the interception and tracking of communications including those utilising existing and future communications systems;
   - subject to proper safeguards, the utility of undercover operations;
   - the use of special investigative tools, including informants; and
   - the relevance of licensing information as a tool for investigating cyber financial crime.

c. In the context of legal issues:
   - the application to cyber and other electronic-media records of existing rules covering law enforcement access to information;
the need to develop and harmonise laws and regulations governing cyber crimes and cyber activity and the improvement of oversight and enforcement mechanisms;

the desirability of establishing bodies to draft common licensing standards for Internet Service Providers and the adoption of approval procedures for new software applications in the field of Internet gaming;

the need to establish common definitions of legitimate and illegitimate Cyberspace financial activity;

the need to improve mutual legal assistance and letters rogatory procedures, and informal assistance, evidence, and information exchange procedures to ensure their application to cyberspace and to overcome delay and resource problems;

the need to develop rules which will enable criminal proceedings in cyber crime cases to be brought in the most appropriate jurisdiction; and

the need to consider international law and sovereignty issues which arise when computer search techniques result in cross border investigative action.

14. In reaching these conclusions, the Workshop noted and was strongly of the view that national capacities, resources, economic circumstances and training and technical assistance needs had to be taken fully into account in formulating any proposals for further action to be taken by CFATF and Commonwealth member governments.
GLOSSARY

Active-X Control: A software component capable of independent data manipulation through a structured set of commands.

ADSL: Asymmetric Digital Subscriber Line - A protocol used to deliver high bandwidth communications over conventional copper wire telephone networks.

Artificial Intelligence - Artificial Intelligence is defined as the a field of endeavor where computers and software programs are designed to mimic human reasoning and learning processes through the discovery of heuristics (rules) and algorithms that are then used to characterize an uncertain environment.

Bandwidth: The amount of data that can be sent through a given communications circuit per second.

Biometric Identification Devices - Biometric Identification Devices are hardware and software systems which authenticate the identities of human beings through the capture of unique data characterizing physical features of the human body. Examples include images of a person's finger or palm print, a laser-scan of an individual's retina, and a voiceprint.

Caribbean Financial Action Task Force (CFATF) - 23 Member States: The CFATF is the Caribbean affiliate of the FATF. It was established in November 1992 and has adopted the FATF 40 Recommendations and an additional 19 regional recommendations. The CFATF conducts mutual evaluations and typologies exercises similar to those of the FATF. The CFATF continues to be the region's key regional anti-money laundering body. In recognition of its increased scope and pace of activities the EU and the U.S. have made the CFATF the implementing body for a comprehensive five-year training and technical assistance program.

Credit Cards -- Payment instruments that allow a user to pay for goods through funds credited to him/her by a credit card issuing company.

Cryptography -- The science and technology of keeping information secret from unauthorized parties by using a mathematical code or a cipher.

Cyberpayments - Cyberpayments are payments instruments utilizing advanced computing and network communications techniques to transfer monetary value between businesses, consumers, and financial service providers. Examples of Cyberpayment instruments include stored value-type smart cards, Internet-based E-cash systems, and hybrid payment systems with both network and smart card features.

Debit Cards -- Payment instruments which, when used to pay for an item or gain access to cash, debit a funds-holding account at a financial institution up to the users available balance.

Denomination Limits -- The upper limit beyond which value can no longer be added to a Cyberpayment instrument - typically discussed in the context of Smart Cards.

Digital Links - See Digital Signatures below.
Digital Signatures -- A Digital Signature is a label attached to email, data, or electronic value within a network that authenticates the identities of particular individuals or entities.

Disintermediation -- The potential of Cyberpayments systems to allow "non-intermediated" transfers of value to take place without the involvement of an identifiable third party subject to legal and regulatory oversight.

The Egmont Group -- The Egmont Group is an international organization formed in June 1995 by 24 countries and 8 international organizations. It is comprised of Financial Intelligence Units (see below) and focuses on coordinating member states efforts at combating international money laundering.

Financial Action Task Force (FATF) -- The FATF, an inter-governmental body, is recognized as the leading organization that addresses the global problem of money laundering. Formed by the G-7 Economic Summit in 1989, the FATF is comprised of 26 jurisdictions, and two international organizations, representing the world’s major financial centers. It is dedicated to promoting the development of effective anti-money laundering controls and facilitates enhanced international cooperation among its members and around the world.

Financial Intelligence Unit (FIU) -- FIUs have been established in various countries around the world to detect criminal abuse of the financial system, ensure adherence to laws against financial crime and protect the banking community. FinCEN is a model of an FIU and others exist in such countries as Great Britain, France, Belgium, the Netherlands, Argentina, and Australia.

FinCEN (Financial Crimes Enforcement Network) -- An agency of the U.S. Treasury Department established in 1990 by Treasury Order 105-08. FinCEN is a financial intelligence unit (FIU) which supports financial investigations, develops and administers anti-money laundering regulations, and promotes international coordination and cooperation to fight money laundering.

Global Information Infrastructure (GII) -- The term used to describe the convergence of local and wide area information networks fostered by the emergence of open standards in networks. Within the GII, common protocols allowing geographically separated dissimilar computer networks to interact with one another and exchange information (text, pictures, audio, or video) in a digital form. The redundant nature of the GII permits communications between networks to be routed around malfunctioning systems.

Integration -- The final phase of the three generic phases of money laundering where a criminal, having successfully concealed the origin of illicit proceeds, desires to use the money for legitimate financial purposes such as business or real estate purchases. To facilitate such transactions, the laundered funds may be integrated with money from legitimate commercial activities. The illicit funds thus take on the appearance of legitimacy.

Intelligent Software Agents -- Software programs designed to accomplish tasks independent of user intervention. In a network environment such programs may seek out patterns in network traffic or in network usage by identifiable actors and aggregate this information into a structured presentation suitable for law enforcement use.
**Interpol** - The International Criminal Police Organization (Interpol) was founded to promote the widest possible mutual assistance among all law enforcement authorities, within the limits of the laws of member states. Interpol has 176 member states and a headquarters linked together by a secure encrypted network.

**Internet Banking** - The delivery of traditional banking services over the Internet. Internet banking provides basic financial services such as funds transfers, bill paying and purchases of financial instruments to customers through an online connection.

**Internet Gambling** - The delivery of gaming opportunities through the Internet. These activities involve the playing of games of chance through a site of the world wide web, as well as the delivery of bookmaking services to gamblers connected through an online service.

**ISDN:** Integrated Services Digital Network - A hardware and software system for the delivery of high bandwidth data communications over fiber optic networks.

**Key Escrow** -- Key Escrow encryption plans envision the use of a trusted agent or third party (governmental or non-governmental in nature) which would store an extra copy of a private key used in a Public-key encryption implementation. Under legal and administrative guidelines such a key would be made available to authorized agencies (e.g., Law Enforcement Agencies) for investigative purposes. With access to private keys, authorized agencies would be able to decrypt cyphertext (the encrypted information) containing potentially valuable data.

**Key Recovery** -- Key Recovery encryption plans envision the filing - by creators of encryption products - of plans for the recovery of private keys used in implementations of Public Key encryption. Such recovery plans would be deposited with the Department of Justice, and would allow - under court order - Law Enforcement and other authorized government agencies to gain access to procedures and techniques which would allow the recovery of a Private Key used in a Public Key encryption system. This proposal originated after widespread criticism of earlier Key Escrow proposals. Specific implementations of Key Recovery have yet to be offered.

**Layering** -- The second phase of the three generic phases of money laundering where the criminal obscures the trail left by illicit proceeds (aka "dirty money"). The objective of this phase is to carry out a series of financial transactions in order to build layers between the funds and their illicit source. For example, a series of bank-to-bank wire transfers would constitute layering. Activities of this nature, especially when they involve funds transfers between tax haven and bank secrecy jurisdictions, make it very difficult for investigators to follow the trail of money.

**Letters Rogatory** - A request by one court of another court in an independent jurisdiction, that a witness be examined upon interrogatories sent with the request.

**Money Laundering** - The process of transforming the proceeds of illegal activities into legitimate wealth. Another definition often cited is “the process by which one conceals the existence, legal source, or illegal application of income, and then disguises that income to make it appear legitimate.”

**Mutual Legal Assistance Treaty** - A binding agreement between two countries to cooperate on a request for information in criminal investigations. Such information would include bank
account information or information that would be provided in the deposition of a witness in a criminal prosecution.

**Network-borne Tracking Device** -- A Network-borne Tracking Device is a software or hardware system designed to trace data as it transits a packet-switched network. Systems in this category include network analyzers used by systems administrators to oversee local area networks, and “sniffers” designed to detect the origins of packets within a network.

**Offshore**: Foreign or overseas jurisdictions.

**Organization of American States/Inter-American Drug Abuse Control Commission (OAS/CICAD) - 29 Members:** CICAD is the specialized OAS body dealing with drugs and money laundering control which was established in 1986. CICAD reconvened its Experts Group on Money Laundering in 1996 to deal with the issue of implementation of the Summit of Americas Communiqué Plan of Action against money laundering. OAS progress on money laundering has increased significantly in the Experts Group which is also revising the 1992 OAS model regulations and is developing a comprehensive anti-money laundering training and technical assistance program for regulators, law enforcement, and FIU.

**Payer Anonymity** -- Smart Card and Internet-based payments systems allow a high degree of anonymity for the payer (or initiator) of transfers of value in a transaction. Anonymity may allow criminals to conceal their identities in Cyberpayments value transfers, thus facilitating money laundering. Restrictions on anonymity in SMARTCARD systems will assist law enforcement in tracking money laundering, but also involve difficult issues of privacy and security.

**Peer-to-Peer Value Transfers** -- Peer to Peer Value Transfers are a facility enabled by Smart Cards and Internet-based Cyberpayments systems that allows the holder of a Smart Card or Cyberpayments “wallet” to transfer some of its value to another Smart Card or Cyberpayments “wallet” holder. These value transfers are disintermediated, that is, they do not involve an identifiable third party subject to regulatory and law enforcement oversight.

**Placement** -- The initial phase of the three generic phases of money laundering where cash enters the financial system. For example, placement occurs when illicit cash is deposited in a bank or money orders are purchased using cash from a criminal enterprise. It is during the placement stage that illicit funds are most vulnerable to detection by law enforcement authorities.

**Private-Key** -- the private (secret) key associated with a person or entity’s public key or a public key encryption system.

**Public Switched Network (PSN)** -- the term commonly used in the U.S. telecommunications industry and elsewhere for the public telephone system.

**Public-Key Encryption** -- A system of encryption utilizing a public key to authenticate the identity of an actor sending or receiving information through an encryption-enabled communications system. Public key encryption uses separate keys to encrypt and decrypt messages meant for an authorized user. The public key is widely distributed and is used to encrypt messages meant for the public key’s legitimate holder. The holder (owner of the public key) can then decrypt a message using a secret private key secure in the knowledge that the
message had not been altered in transit. Public key encryption systems also allow for the authentication of the identity of the sender in that they can be adjusted to include information regarding the identity of the sending party.

**Purse Integrity** -- The integrity of the “holder” of value contained within a Smart Card payment instrument. Because Smart Cards typically use a combined Public Key - Private Key encryption system to store value, these purses are subject to the vulnerabilities of established encryption systems.

**SET** -- SET stands for the Secure Electronic Transactions encryption protocol for securing electronic commerce. This standard was created collaboratively by Visa International, IBM, MasterCard, Microsoft, and other large corporations.

**Stale-dating of Smart Card Value** -- A concept for manipulating the “aging” of stored value within Cyberpayment instruments for the purposes of regulatory and law enforcement oversight.

**Smart cards** -- Smart cards are electronic instruments with the form factor of a conventional credit or debit card. These cards have embedded microchips that enable them to hold sensitive digital information. Smart cards are currently under development as replacements for credit and debit cards, and as a new stored value vehicle enabling the storage of electronic currency within the card itself.

**Sniffers** -- Sniffers are software programs that allow for the covert gathering of password and other information from computers as they are operated in an authorized user environment. Hackers typically use sniffers to detect passwords in normal network traffic, and then seek to gain unauthorized access to the information systems so compromised.

**Value Tagging** -- A concept for tagging the value in a stored value instrument so that it can be tracked as it transits a Cyberpayment infrastructure.