International Guide to Combating Cybercrime

American Bar Association
Privacy & Computer Crime Committee
Section of Science & Technology Law

Jody R. Westby, Project Chair & Editor
SUMMARY OF CONTENTS

Preface ix

Abbreviations xiii

List of Participants xvii

Executive Summary xxi

Introduction 1

CHAPTER 1

Cybercrime Laws 11
  I. Introduction 11
  II. Laws on Crimes against Computer Systems 16
  III. Laws on Crimes against Communications Systems 26
  IV. Crimes Facilitated by Computers and the Internet 34
  V. Authentication and Security Laws 39
  VI. Conclusion 40

CHAPTER 2

Jurisdiction 41
  I. Introduction 41
  II. International Legal Assistance 43
  III. Jurisdictional Considerations and Conflicts of Laws 49
  IV. What Is Being Done to Address Cybercrime-Related Jurisdictional Concerns? 59
  V. Conclusion 79

CHAPTER 3

Law Enforcement 81
  I. Introduction 81
  II. Impact of Cybercrime on Law Enforcement 84
CHAPTER 4
Search and Seizure    123
I. Introduction    123
II. Overview of Types of Search and Seizure    124
III. Practical Considerations for Immediate Search and Seizure
     of Digitally Stored Evidence    127
IV. Legal Considerations    135
V. Conclusion    163

CHAPTER 5
Public/Private Cooperation    165
I. Introduction    165
II. Preliminary Issues    168
III. Analysis    173
IV. Some Components of Cyber Security Cooperation    184
V. International Efforts to Stimulate Private and Public Sector
     Cooperation to Combat Cybercrime    188
VI. Additional Resources    194
VII. Conclusion    197

Bibliography & Additional Resources    199
I. Bibliography    199
II. Additional Resources    220

Index    227
CONTENTS

Preface ix

Abbreviations xiii

List of Participants xvii

Executive Summary xxi
  A. Introduction xxi
  B. Cybercrime Laws xxii
  C. Jurisdiction xxiv
  D. Law Enforcement xxv
  E. Search and Seizure xxvii
  F. Public/Private Cooperation xxviii

Introduction 1
  A. Background 1
  B. Actions by the Group of Eight and Council of Europe 2
  C. The Opportunity for Developing Countries 5
  D. The Importance of Cybercrime Laws and ICT Security 6
  E. International Cooperation Needed for Global Cybercrime Problems 8
  F. Scope of International Cybercrime Project 9

CHAPTER 1
Cybercrime Laws 11
  I. Introduction 11
    A. Background 11
    B. Chapter Overview 15
  II. Laws on Crimes against Computer Systems 16
    A. Introduction 16
    B. North America—Laws on Crimes against Computer Content and Systems 16
    C. Europe—Laws on Crimes against Computer Systems 21
    D. Asia-Pacific—Laws on Crimes against Computer Systems 24
  III. Laws on Crimes against Communications Systems 26
A. Introduction 26
B. North America—Laws on Crimes against Communication Systems 28
C. Europe—Laws on Crimes against Communication Systems 31
D. Asia-Pacific—Laws on Crimes against Communication Systems 33
IV. Crimes Facilitated by Computers and the Internet 34
   A. Introduction 34
   B. Types of Offenses 35
   C. Responding to Investigatory Challenges 39
V. Authentication and Security Laws 39
VI. Conclusion 40

CHAPTER 2
Jurisdiction 41
I. Introduction 41
   A. Jurisdictional Issues Generally 41
   B. Jurisdictional Issues in Cybercrime Cases 42
   C. Chapter Overview 43
II. International Legal Assistance 43
   A. Introduction 43
   B. Traditional Methods of Securing International Legal Assistance 44
   C. Problems with Traditional Methods in Cybercrime Cases 47
III. Jurisdictional Considerations and Conflicts of Laws 49
   A. Introduction 49
   B. Discussion 50
IV. What Is Being Done to Address Cybercrime-Related Jurisdictional Concerns? 59
   A. Domestic Initiatives 59
   B. Multilateral Initiatives 61
   C. Interjurisdictional Networks and Other Initiatives 72
V. Conclusion 79

CHAPTER 3
Law Enforcement 81
I. Introduction 81
   A. The Impact of the Global Internet on Law Enforcement 81
   B. Redefining Law Enforcement 82
   C. Chapter Overview 84
CHAPTER 5

Public/Private Cooperation 165

I. Introduction 165
   A. Background 166
   B. Chapter Overview 168

II. Preliminary Issues 168
   A. Review Infrastructure 168
   B. Prioritize Critical Sectors 168

III. Analysis 173
   A. Infrastructure Management 173
   B. Information Sharing and Analysis Centers (ISACs) 174
   C. Benefits of Information Sharing 176
   D. Potential Risks of Information Sharing 178
   E. Laws That Impede Information Sharing 181

IV. Some Components of Cyber Security Cooperation 184
   A. Risk Management Approaches 184

V. International Efforts to Stimulate Private and Public Sector
   Cooperation to Combat Cybercrime 188
   A. Activities of Governmental Bodies 188
   B. Activities of Nongovernmental Organizations 191
   C. Selected Activities within Specific Countries 193

VI. Additional Resources 194
   A. Standards-Setting Bodies 194
   B. Security-Related Standards 195
   C. Selected Websites 195

VII. Conclusion 197

Bibliography & Additional Resources 199

I. Bibliography 199
   A. Cases 199
   B. Organizations 200
   C. Reference Materials 204
   D. Statutes and Legal Documents 215

II. Additional Resources 220
   A. Cybercrime 220
   B. Jurisdiction 221
   C. Law Enforcement 221
   D. Search and Seizure 223
   E. Public/Private Cooperation 224
   F. Other 225

Index 227
We are all privileged to live during the Digital Revolution—a time that history will show to be as important, if not more so, than the Renaissance. Information and communication technologies (ICTs) are transforming art, music, cultures, and societies. They are impacting the way we live, learn, work, play, and interact with one another. ICTs are also propelling globalization and affording developed and developing nations alike an equal opportunity to advance their economies and improve their productivity, competitiveness, and trade. However, the benefits of ICTs are being undercut by their use for criminal activity.

Today, the Internet is connected to nearly 200 countries. The very nature of a globally connected network has made it painfully clear that cybercriminal activity cannot be effectively addressed by individual nations or even by a group of industrialized countries. It requires a concerted global effort between industry, government officials, law enforcement, and citizens of all countries.

Since 1995, when the National Science Foundation turned the Internet backbone over to commercial companies, we have gone from a totally unregulated Internet toward one that now is subject to a myriad of laws and regulations set by over 50 national governments and multinational organizations. This developing global legal framework, however, is in its infancy; and inconsistencies, gaps, and voids are most apparent in the area of cybercrime.

Efforts to combat cybercrime are often thwarted because this is the area of law that most developing countries address last, rather than first. Therefore, industrialized nations’ ability to track and prosecute cross-border cyber criminal activities is hindered because of (a) inadequate or nonexistent laws and regulations, (b) a lack of cooperation by inexperienced law enforcement and prosecutors, (c) inexperienced or untrained personnel in the search and seizure of electronic evidence, and (d) little public/private cooperation. In an
interconnected world, the weakest link is everyone’s concern. Clearly, negative uses of technology will significantly reduce the benefits that flow from the use of ICTs—for developed and developing nations.

For developing countries, cybercrime carries a particularly high cost. ICTs can help them make dramatic leaps toward industrialization, but cyber criminal activities conducted within their borders will deter foreign direct investment (FDI), and lax laws will attract criminals seeking a haven for their activities or a safe repository for their data. This means the potential of the Digital Revolution will be diminished for us all.

This project was designed to facilitate the beneficial use of ICTs by all countries and to encourage international cooperation on cybercrime issues. Industrialized nations have taken some initial steps to work together in a coordinated fashion to combat cybercrime, yet little has been done to extend this work or to provide guidance to developing countries. Thus, there is a vast chasm in our ability to deter and prosecute cybercrime.

The lawyers, government personnel, nonprofit staff, university professors, and individuals who came together to create this International Guide to Combating Cybercrime gave selflessly over a ten-month period to produce a manual that would help all stakeholders—companies, governments, organizations, lawyers, judges, police, and citizens—better understand the key aspects of cybercrime. In the true spirit of public private cooperation, these people contributed their time and talent so they might help advance the quality of life in their countries, facilitate global cooperation on cybercrime issues, and help those less fortunate realize the full benefits of ICTs. Not a bad reward for intellectual efforts.

I owe a debt of gratitude to the members of the American Bar Association Privacy & Computer Crime Committee’s International Cybercrime Project. I especially want to thank David Weitzel, Lesia Stangret, Michael Nugent, Francoise Gilbert, Brad Laybourne, Jim Dempsey, Joe Schwerha, Marc Goodman, Dan Hurley, Angie Chen, Ivan Fong, Drew Arena, Barry Steinhardt, Lee Tien, David Sobel, Susan Brenner, Steve Chabinsky, James Savage, Francis Dong, Jessica Milano, and Andrew Downey for their leadership, advice, and devotion to this project—even when their calendars were full. I would like to extend a special note of appreciation to Dave Yee for his tireless efforts in editing the final document when he could have been enjoying delicious freedom after finishing law school and passing the bar.
Lastly, but perhaps most importantly, I am grateful to the ABA staff who generously gave support, encouragement, and resources to the publication of this Guide: Shawn Kaminski, Deborah Douglas, Richard Paszkiet, and Maureen Grey.

Jody R. Westby
Chair, Privacy & Computer Crime Committee
& International Cybercrime Project
ABA Section of Science & Technology Law
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>24/7</td>
<td>24 hours a day, 7 days a week</td>
</tr>
<tr>
<td>ABA</td>
<td>American Bar Association</td>
</tr>
<tr>
<td>AIIP</td>
<td>Agency for Information Infrastructure Protection</td>
</tr>
<tr>
<td>ANSI</td>
<td>American National Standards Institute</td>
</tr>
<tr>
<td>APEC</td>
<td>Asia-Pacific Economic Cooperation</td>
</tr>
<tr>
<td>APEC-TEL</td>
<td>Asia-Pacific Economic Cooperation Telecommunications and Information Working Group</td>
</tr>
<tr>
<td>ASP</td>
<td>Application Service Provider</td>
</tr>
<tr>
<td>AUSA</td>
<td>Assistant U.S. Attorney (U.S. Department of Justice)</td>
</tr>
<tr>
<td>AUSCERT</td>
<td>Australian Computer Emergency Response Team</td>
</tr>
<tr>
<td>BIS</td>
<td>Bank for International Settlements</td>
</tr>
<tr>
<td>BSA</td>
<td>Business Software Alliance</td>
</tr>
<tr>
<td>CCC</td>
<td>Canadian Criminal Cases</td>
</tr>
<tr>
<td>CCIPS</td>
<td>Computer Crime and Intellectual Property Section (U.S. Department of Justice)</td>
</tr>
<tr>
<td>CD</td>
<td>Compact Disk</td>
</tr>
<tr>
<td>CEO</td>
<td>Chief Executive Officer</td>
</tr>
<tr>
<td>cert.</td>
<td>Certiorari (review by the U.S. Supreme Court)</td>
</tr>
<tr>
<td>CERT</td>
<td>Computer Emergency Response Team (U.S.)</td>
</tr>
<tr>
<td>CFAA</td>
<td>Computer Fraud and Abuse Act (U.S.)</td>
</tr>
<tr>
<td>CHIP</td>
<td>Computer Hacking and Intellectual Property Unit (U.S. Department of Justice)</td>
</tr>
<tr>
<td>CIAO</td>
<td>Critical Infrastructure Assurance Office (U.S.)</td>
</tr>
<tr>
<td>CICTE</td>
<td>Inter-American Committee Against Terrorism (OAS)</td>
</tr>
<tr>
<td>CICP</td>
<td>Centre for International Crime Prevention (UN)</td>
</tr>
<tr>
<td>Cir.</td>
<td>Circuit, as Circuit Court (U.S.)</td>
</tr>
<tr>
<td>CMA</td>
<td>Computer Misuse Act of 1990 (U.K.)</td>
</tr>
<tr>
<td>CoE</td>
<td>Council of Europe</td>
</tr>
<tr>
<td>CSI</td>
<td>Computer Security Institute</td>
</tr>
<tr>
<td>CTC</td>
<td>Communications and Telecommunications Coordinator (U.S. Department of Justice)</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>DDOS</td>
<td>Distributed Denial of Service</td>
</tr>
<tr>
<td>DEA</td>
<td>Drug Enforcement Administration (U.S.)</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard</td>
</tr>
<tr>
<td>DOJ</td>
<td>Department of Justice (U.S.)</td>
</tr>
<tr>
<td>DSL</td>
<td>Digital Subscriber Line</td>
</tr>
<tr>
<td>DSS/SHS</td>
<td>Digital Signature Standard and Secure Hash Standard</td>
</tr>
<tr>
<td>EBRD</td>
<td>European Bank of Reconstruction and Development</td>
</tr>
<tr>
<td>EC</td>
<td>European Commission</td>
</tr>
<tr>
<td>ECHR</td>
<td>European Convention on Human Rights</td>
</tr>
<tr>
<td>ECtHR</td>
<td>European Court on Human Rights</td>
</tr>
<tr>
<td>ECPA</td>
<td>Electronic Communications Privacy Act</td>
</tr>
<tr>
<td>ECSAP</td>
<td>Electronic Crimes Special Agent Program (U.S.)</td>
</tr>
<tr>
<td>EHHR</td>
<td>European Human Rights Reporter</td>
</tr>
<tr>
<td>EJN</td>
<td>European Judicial Network</td>
</tr>
<tr>
<td>ELO</td>
<td>European Liaison Officer (Europol)</td>
</tr>
<tr>
<td>ENU</td>
<td>Europol National Unit</td>
</tr>
<tr>
<td>E-SIGN</td>
<td>Electronic Signatures in Global and National Commerce Act (U.S.)</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>EUROPOL</td>
<td>European Police Office</td>
</tr>
<tr>
<td>F.2d</td>
<td>Federal Reporter (Second Edition) (U.S. federal appellate court decisions)</td>
</tr>
<tr>
<td>FATF</td>
<td>Financial Action Task Force</td>
</tr>
<tr>
<td>FBI</td>
<td>Federal Bureau of Investigation (U.S.)</td>
</tr>
<tr>
<td>FDCA</td>
<td>Food, Drug &amp; Cosmetic Act (U.S.)</td>
</tr>
<tr>
<td>FDI</td>
<td>Foreign Direct Investment</td>
</tr>
<tr>
<td>FedCIRC</td>
<td>Federal Computer Incident Response Center (U.S.)</td>
</tr>
<tr>
<td>FIRST</td>
<td>Forum of Incident Response and Security Team</td>
</tr>
<tr>
<td>FLETC</td>
<td>Federal Law Enforcement Training Center (U.S.)</td>
</tr>
<tr>
<td>FOIA</td>
<td>Freedom of Information Act (U.S.)</td>
</tr>
<tr>
<td>FS-ISAC</td>
<td>Financial Services Information Sharing &amp; Analysis Center (U.S.)</td>
</tr>
<tr>
<td>F.Supp.</td>
<td>Federal Supplement (U.S. federal trial court cases)</td>
</tr>
<tr>
<td>FTC</td>
<td>Federal Trade Commission (U.S.)</td>
</tr>
<tr>
<td>G-8</td>
<td>Group of Eight</td>
</tr>
<tr>
<td>GAO</td>
<td>General Accounting Office (U.S.)</td>
</tr>
<tr>
<td>GBD-e</td>
<td>Global Business Dialogue on Electronic Commerce</td>
</tr>
<tr>
<td>GIIC</td>
<td>Global Information Infrastructure Commission</td>
</tr>
<tr>
<td>GIP</td>
<td>Global Internet Project</td>
</tr>
<tr>
<td>GLBA</td>
<td>Gramm-Leach-Bliley Act (U.S.)</td>
</tr>
<tr>
<td>HIPAA</td>
<td>Health Insurance Portability and Accountability Act (U.S.)</td>
</tr>
<tr>
<td>HS Act</td>
<td>Homeland Security Act of 2002 (U.S.)</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>IADB</td>
<td>Inter-American Development Bank</td>
</tr>
<tr>
<td>ICC</td>
<td>International Chamber of Commerce</td>
</tr>
<tr>
<td>ICCP</td>
<td>Information, Computer and Communications Policy Committee (OECD)</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communication Technology</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IIA</td>
<td>The Institute of Internal Auditors</td>
</tr>
<tr>
<td>ILPF</td>
<td>Internet Law and Policy Forum</td>
</tr>
<tr>
<td>IMSN</td>
<td>International Marketing Supervision Network</td>
</tr>
<tr>
<td>INCB</td>
<td>International Narcotics Control Board (UN)</td>
</tr>
<tr>
<td>INL</td>
<td>International Narcotics and Law Enforcement Affairs (U.S. Department of State)</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>ISAC</td>
<td>Information Sharing &amp; Analysis Center</td>
</tr>
<tr>
<td>ISO</td>
<td>International Standards Organization</td>
</tr>
<tr>
<td>ISOC</td>
<td>Internet Society</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>ISTWG</td>
<td>Industrial Science and Technology Working Group (APEC)</td>
</tr>
<tr>
<td>ITAA</td>
<td>Information Technology Association of America</td>
</tr>
<tr>
<td>ITC</td>
<td>Information Technology Crime</td>
</tr>
<tr>
<td>IT-ISAC</td>
<td>Information Technology Information Sharing &amp; Analysis Center</td>
</tr>
<tr>
<td>ITU</td>
<td>International Telecommunications Union</td>
</tr>
<tr>
<td>LINX</td>
<td>London Internet Exchange</td>
</tr>
<tr>
<td>MLAT</td>
<td>Mutual Legal Assistance Treaty</td>
</tr>
<tr>
<td>MOU</td>
<td>Memorandum of Understanding</td>
</tr>
<tr>
<td>NAC</td>
<td>National Advocacy Center (U.S.)</td>
</tr>
<tr>
<td>NCB</td>
<td>National Central Bureau (Interpol)</td>
</tr>
<tr>
<td>NCTP</td>
<td>National Cybercrime Training Partnership (U.S.)</td>
</tr>
<tr>
<td>N.D.</td>
<td>Northern District (U.S. federal district court region)</td>
</tr>
<tr>
<td>NDAA</td>
<td>National District Attorneys Association</td>
</tr>
<tr>
<td>NIJ</td>
<td>National Institute of Justice (U.S.)</td>
</tr>
<tr>
<td>NIPC</td>
<td>National Infrastructure Protection Center (U.S.)</td>
</tr>
<tr>
<td>NISCC</td>
<td>National Infrastructure Security Coordinating Center (U.K.)</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology (U.S.)</td>
</tr>
<tr>
<td>NGO</td>
<td>Non-Governmental Organization</td>
</tr>
<tr>
<td>NOIE</td>
<td>National Office for Information Economy (Australia)</td>
</tr>
<tr>
<td>NSTAC</td>
<td>National Security Telecommunications Advisory Committee (U.S.)</td>
</tr>
<tr>
<td>NYECTF</td>
<td>New York Electronic Crimes Task Force (U.S.)</td>
</tr>
<tr>
<td>OAS</td>
<td>Organization of American States</td>
</tr>
</tbody>
</table>
Abbreviations

OCIPEP  Office of Critical Infrastructure Protection and Emergency Preparedness (Canada)
OECD  Organization for Economic Cooperation & Development
OIA  Office of Internal Affairs (Criminal Division, U.S. Department of Justice)
OLAF  European Anti-Fraud Office
OPDAT  Overseas Prosecutorial Development Assistance and Training Unit (U.S. Department of Justice)
PDA  Personal Data Assistant
PKI  Public Key Infrastructure
RAM  Random Access Memory
RCMP  Royal Canadian Mounted Police
RIPA  Regulation of Investigatory Powers Act (U.K.)
RMI  Records Management Institute (Canada)
SCR  Supreme Court Reports (Canada)
SEC  Securities and Exchange Commission (U.S.)
SIIOC  Strategic Information and Operations Center (U.S.)
SME  Small and Medium-Sized Enterprise
TECS  The Europol Computer System
TELMIN 5 Ministers for the Telecommunications and Information Industries—5th Meeting (APEC)
U.K.  United Kingdom
UL  Underwriters Laboratory
UN  United Nations
UNCITRAL  UN Commission on International Trade Law
UNCJIN  UN Crime and Justice Information Network
UNICRI  UN Interregional Criminal Justice and Research Institute
U.S.  United States of America
USAID  U.S. Agency for International Development
USA  Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (U.S.)
USCS  United States Customs Service
USSS  United States Secret Service
W3C  World Wide Web Consortium
W.D.  Western District (U.S. federal district court region)
WITSA  World Information Technology and Services Alliance
WPISP  Working Party on Information Security and Privacy (OECD)
WTO  World Trade Organization
LIST OF PARTICIPANTS

American Bar Association
Section of Science & Technology Law
Privacy & Computer Crime Committee

INTERNATIONAL CYBERCRIME PROJECT

The following participants, although not all members of the ABA, provided information and assistance in the development of the International Guide to Combating Cybercrime. The statements and views contained in the Guide are not necessarily endorsed by them or their employers.

Drew C. Arena
Susan Axelrod
Ian Ballon
Michael Bennett
Alain Bensoussan
Harish Bhatt
Susan Brenner
Rico Calleja
Elaine Cassel
Steven Chabinsky
Angeline G. Chen
Paul Coggins
M. Evan Corcoran
George E. Curtis
James X. Dempsey
Francis H. Dong

Verizon Communications
New York County District Attorney’s Office
Manatt, Phelps & Phillips
Cabinet Alain Bensoussan
SingleSignOn.Net, Inc.
University of Dayton School of Law
McDermott, Will & Emery
Law Office of Elaine Cassel
FBI & National Infrastructure Protection Center
International Launch Services (Lockheed Martin)
Fish & Richardson
Wiley, Rein & Fielding
Economic Crime Investigative Institute
Center for Democracy & Technology
DoMo Associates
<table>
<thead>
<tr>
<th>Name</th>
<th>Organization/Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>Andrew Downey</td>
<td>Law Offices of Richard L. Field</td>
</tr>
<tr>
<td>Richard L. Field</td>
<td>Law Offices of Stephen L. Ganis</td>
</tr>
<tr>
<td>Ivan Fong</td>
<td>General Electric Company</td>
</tr>
<tr>
<td>Stephen L. Ganis</td>
<td>Gray Cary</td>
</tr>
<tr>
<td>Francoise Gilbert</td>
<td>Federal Deposit Insurance Corporation</td>
</tr>
<tr>
<td>Edward F.X. Gilbride</td>
<td>Granite Intelligence</td>
</tr>
<tr>
<td>Marc D. Goodman</td>
<td>The Sam Nunn School of International Affairs &amp; the College of Computing, Georgia Institute of Technology</td>
</tr>
<tr>
<td>Seymour E. Goodman</td>
<td>The Sam Nunn School of International Affairs &amp; the College of Computing, Georgia Institute of Technology</td>
</tr>
<tr>
<td>Gary R. Gordon</td>
<td>Economic Crime Investigative Institute</td>
</tr>
<tr>
<td>Janine Hiller</td>
<td>Virginia Tech</td>
</tr>
<tr>
<td>Virginia Holden</td>
<td>McDermott, Will &amp; Emery</td>
</tr>
<tr>
<td>Rick Hornbeck</td>
<td>Hornbeck Consulting</td>
</tr>
<tr>
<td>Daniel C. Hurley, Jr.</td>
<td>NTIA, U.S. Department of Commerce</td>
</tr>
<tr>
<td>Mary Ellen F. Hurley</td>
<td>D.C. Court of Appeals</td>
</tr>
<tr>
<td>Frank J. Johnson, Jr.</td>
<td>Sheppard, Mullin, Richter &amp; Hampton</td>
</tr>
<tr>
<td>Tom Kellerman</td>
<td>The World Bank</td>
</tr>
<tr>
<td>Susan Koeppen</td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td>James W. Lacey, Jr.</td>
<td>U.S. National Central Bureau, Interpol (former position)</td>
</tr>
<tr>
<td>David Lanham</td>
<td>University of Melbourne</td>
</tr>
<tr>
<td>Brad Laybourne</td>
<td>Gray Cary</td>
</tr>
<tr>
<td>Michael Ledgett</td>
<td>Aird &amp; Berlis</td>
</tr>
<tr>
<td>Edward P. Malloy</td>
<td>U.S. Agency for International Development</td>
</tr>
<tr>
<td>Monique Mattei</td>
<td>State of Connecticut</td>
</tr>
<tr>
<td>Ellen C. McBarnette</td>
<td>American Bar Association</td>
</tr>
<tr>
<td>Jonathan Reed Metzger</td>
<td>Academy for Educational Development</td>
</tr>
<tr>
<td>Jessica A. Milano</td>
<td>DoMo Associates</td>
</tr>
<tr>
<td>Charles L. Mudd, Jr.</td>
<td>Privacy Resolutions P.C.</td>
</tr>
<tr>
<td>Timothy J. Nagle</td>
<td>TRW Systems</td>
</tr>
<tr>
<td>Michael Nugent</td>
<td>Heller Ehrman</td>
</tr>
<tr>
<td>Andy Ozment</td>
<td>Georgia Tech College of Computing</td>
</tr>
<tr>
<td>Ronald E. Plesco, Jr.</td>
<td>GW Solutions</td>
</tr>
<tr>
<td>Virginie Prat</td>
<td>Cabinet Alain Bensoussan</td>
</tr>
<tr>
<td>Philip Rees</td>
<td>McDermott, Will &amp; Emery</td>
</tr>
<tr>
<td>Michele J. Rubenstein</td>
<td>solutions4networks</td>
</tr>
<tr>
<td>Nina Santucci</td>
<td>Windermere Corporation</td>
</tr>
<tr>
<td>James Savage</td>
<td>U.S. Secret Service</td>
</tr>
<tr>
<td>Paul H. Schwartz</td>
<td>Cooley Godward</td>
</tr>
</tbody>
</table>
## List of Participants

<table>
<thead>
<tr>
<th>Name</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Joseph J. Schwerha, IV</td>
<td>Office of the District Attorney for Washington County</td>
</tr>
<tr>
<td>Satwiksai Seshasai</td>
<td>Massachusetts Institute of Technology (student)</td>
</tr>
<tr>
<td>Sanyin Siang</td>
<td>American Association for the Advancement of Science</td>
</tr>
<tr>
<td>Christopher Sloan</td>
<td>Liberty Mutual Insurance Company</td>
</tr>
<tr>
<td>Thomas J. Smedinghoff</td>
<td>Baker &amp; McKenzie</td>
</tr>
<tr>
<td>Philip J. Smith</td>
<td>TrustWave Corporation</td>
</tr>
<tr>
<td>David Sobel</td>
<td>Electronic Privacy Information Center</td>
</tr>
<tr>
<td>Clifford S. Stanford</td>
<td>Federal Reserve Bank of Atlanta</td>
</tr>
<tr>
<td>Lesia Stangret</td>
<td>Office of the Secretary of State (Asia-Pacific), Canada</td>
</tr>
<tr>
<td>Barry Steinhardt</td>
<td>American Civil Liberties Union</td>
</tr>
<tr>
<td>Lowell Thomas</td>
<td>Verizon Communications</td>
</tr>
<tr>
<td>Sandra Thompson</td>
<td>Fish &amp; Associates</td>
</tr>
<tr>
<td>Lee Tien</td>
<td>Electronic Frontier Foundation</td>
</tr>
<tr>
<td>James Vaules</td>
<td>National Fraud Center</td>
</tr>
<tr>
<td>Susan Vernon</td>
<td>Heller Ehrman White &amp; McAuliffe</td>
</tr>
<tr>
<td>Sophia Vicksman</td>
<td>Federal Reserve Bank—New York</td>
</tr>
<tr>
<td>Dennis Walters</td>
<td>National Fraud Center</td>
</tr>
<tr>
<td>David S. Weitzel</td>
<td>Mitretek Systems</td>
</tr>
<tr>
<td>Jody R. Westby</td>
<td>The Work-IT Group</td>
</tr>
<tr>
<td>Wayne P. Williams</td>
<td>National White Collar Crime Center</td>
</tr>
<tr>
<td>Norman A. Willox, Jr.</td>
<td>LexisNexis</td>
</tr>
<tr>
<td>Amy Worlton</td>
<td>Wiley, Rein &amp; Fielding</td>
</tr>
<tr>
<td>Orlie Yaniv</td>
<td>U.S. Department of Defense, C3I</td>
</tr>
<tr>
<td>Matthew E. Yarbrough</td>
<td>Fish &amp; Richardson</td>
</tr>
<tr>
<td>David K. Yee</td>
<td>Willamette University College of Law (student)</td>
</tr>
</tbody>
</table>

### Project Leadership

**Project Chair**
- Jody R. Westby

**Chair, Cybercrime Working Group**
- Michael Nugent

**Co-Chair, Jurisdictional Working Group**
- Francoise Gilbert

**Co-Chair, Jurisdictional Working Group**
- Lesia Stangret

**Co-Chair, Law Enforcement Working Group**
- Harish Bhatt

**Co-Chair, Law Enforcement Working Group**
- Marc Goodman

**Co-Chair, Electronic Search & Seizure Working Group**
- Joseph J. Schwerha, IV

**Co-Chair, Electronic Search & Seizure Working Group**
- James X. Dempsey
xx    LIST OF PARTICIPANTS

Co-Chair, Public/Private Cooperation  Working Group  Daniel C. Hurley, Jr.
Co-Chair, Public/Private Cooperation  Working Group  Angeline G. Chen
Co-Chair, Editing Committee  David S. Weitzel
Co-Chair, Editing Committee  Lesia Stangret

Organizations with Participating Personnel1
The ABA wishes to acknowledge the following organizations that provided assistance to this Project. The statements and views contained in the Guide are not necessarily endorsed by them or their personnel.

American Association for the Advancement of Science
American Civil Liberties Union
Center for Democracy & Technology
Economic Crime Investigative Institute
Electronic Frontier Foundation
Electronic Privacy Information Center
Federal Bureau of Investigation, Cyber Division
Federal Deposit Insurance Corporation
George Mason University
Georgia Institute of Technology—Sam Nunn School of International Affairs & Georgia Tech Information Security Center
Interpol, U.S. National Central Bureau
LexisNexis
National Fraud Center
National Infrastructure Protection Center
National White Collar Crime Center
Pennsylvania State Police
State of Connecticut, Computer Crimes & Electronic Evidence Unit
U.S. Agency for International Development
U.S. Customs Cybersmuggling Center
U.S. Department of Commerce, NTIA
U.S. Department of Defense, C3I
U.S. Secret Service, Financial Crimes
The World Bank

1Personnel from additional U.S. Government agencies and departments participated in this Project, but requested that they and their agencies or departments not be identified.
Executive Summary

A. INTRODUCTION

With nearly 200 countries connected to the Internet, cybercrime has become a global issue that requires the full participation and cooperation of the public and private sectors in all countries, including the 180 developing countries around the globe. A major component of information and infrastructure security is a nation’s ability to deter, detect, investigate, and prosecute cyber criminal activities. Industrialized nations and multinational organizations have taken significant steps toward combating cybercrime. The glaring gaps in combating cybercrime to date are (1) inadequate international coordination and (2) woefully deficient legal frameworks and organizational capacity in developing countries. The American Bar Association’s (ABA) International Cybercrime Project extends the work of the G-8, Council of Europe (CoE), and other industrialized nations regarding cybercrime to developing countries. The project was designed to bring together ABA members and key stakeholders from government, industry, nongovernmental organizations (NGOs), and academia to address issues in five areas important to combating cybercrime. The International Guide to Combating Cybercrime is intended to serve as a manual for developed and developing countries alike to help them (1) create effective cybercrime laws, (2) handle jurisdictional issues, (3) cooperate in international investigations, (4) develop acceptable practices for the search and seizure of electronic evidence, and (5) establish effective public/private sector interaction.
By explaining the importance of these issues, the ABA Privacy and Computer Crime Committee believes this Project will:

■ Help developing countries attract foreign direct investment and offshore technology operations, and bring the economic and social benefits of technology to their people.
■ Promote international cooperation and coordination in combating cybercrime and encourage the establishment of public and private sector structures necessary to share resources and effectively deal with these issues.
■ Help government officials, industry, citizens, academia, and nongovernmental organizations understand their role in combating cybercrime.

B. CYBERCRIME LAWS

Cybercrime laws deter cyber criminal activities and make these offenses punishable, but they vary in form as much as cybercrime itself. Industrialized nations have enacted laws protecting computer and communications systems and the data residing in and transiting these systems.

Generally, these cybercrime laws apply to:

■ Use of computers and the Internet for illegal purposes: viruses, hacking, unauthorized access.
■ Crimes against communication systems.
■ Crimes facilitated by the use of a computer.
■ Wiretap, pen register, and trap-and-trace laws to protect privacy and facilitate investigations.

While some countries, such as the United States, have special provisions for unauthorized actions involving “protected computers” (computers or systems used by financial institutions or the government, or involved in interstate or foreign commerce), other countries do not make this distinction. In most developed countries, cybercrimes are considered criminal offenses and are punishable by prison terms and/or fines. In some instances, civil liability may also be attached.

Industrialized countries have also updated their criminal codes to ensure statutes can be applied by diligent law enforcement authorities and government prosecutors to traditional crimes committed in new ways through computers and the Internet. Nations at the forefront of retooling their criminal legal systems to combat cybercrime have
supplemented these efforts with additional laws and policies promoting electronic authentication and the use of encryption and relaxing controls for import and export of encryption devices and software.

One of the challenges countries face is keeping their computer crime laws up to date. Cybercrime laws are constantly evolving with new technological capabilities and criminal innovation to address new forms of computer crime, new types of criminals, and emerging concerns within the law enforcement community. Also, with improvements in information and communications technology (ICT) throughout the world, making computer crime a seemingly borderless crime, crimes by and against foreign computer systems have proliferated. Nations have responded to transborder cybercrime by modifying their criminal codes to allow for jurisdiction over, and prosecution of, individuals and organizations committing crimes from one country against computers located in another. Finally, as the global legal and regulatory framework develops for e-commerce and security issues, it is generally accepted that online conduct should be treated no differently than offline conduct. In other words, laws should be technologically neutral and based upon the act rather than the technology used to commit the act.

Developing countries are making headway. In seeking to demonstrate the integrity of their computing and information infrastructures and to respond to the accelerating concerns of industrialized nations as expressed through the Organization for Economic Cooperation and Development (OECD), the Financial Action Task Force (FATF), and the Bank for International Settlements (BIS), developing nations have increasingly adopted and improved their computer crime laws to emulate the laws of more developed nations. Modeling cybercrime laws after those put forth by multinational organizations and countries that are leaders in commerce is the correct approach. Developing countries should take a global perspective when creating a legal and regulatory framework regarding ICTs. They are encouraged to participate in United Nations (UN) activities in this regard, to join multinational organizations, and to become global players as these issues are discussed and debated and new global legal structures are formed. Countries in line for accession into the European Union (EU) should, of course, closely monitor EU developments in the cybercrime arena. Likewise, countries in the Asia-Pacific region should be mindful of directions from the Asia-Pacific Economic Cooperation (APEC) forum. The leading multinational organizations involved in the ICT legal arena are the UN, OECD, World Trade Organization
(WTO), EU, CoE, and APEC. Although not a multinational entity, the United States is also influential regarding ICT legal/regulatory issues.

C. JURISDICTION

Jurisdictional issues present some of the greatest challenges to combating cybercrime. The Internet has made it possible for a cyber criminal to be physically located in one country, weave an attack through multiple countries and computers, and store the evidence of the crime on servers in yet another country. Victims may be all over the globe. While the Internet is borderless, the investigation and prosecution of electronic crimes is not; the borders of sovereign states and their legal systems must be recognized. One of the most complex jurisdictional issues occurs when substantive or procedural laws of the involved countries conflict.

The international community has developed long-standing methods for obtaining and providing legal assistance. The most common are the Letters Rogatory process and Mutual Legal Assistance Treaties (MLATs), often negotiated on a country-to-country basis. These processes are time-consuming and often contain limitations on what assistance may be obtained. Dual criminality requirements can be especially problematic. Where the goal is to prosecute an accused located abroad, there also needs to be a way to secure that person’s extradition. Here, too, countries negotiate extradition treaties that govern how to make and respond to extradition requests. Many countries, however, will not extradite their own citizens. Although most of the jurisdictional issues raised in cybercrime cases are not new, the Internet complicates them and increasingly brings them to the forefront.

A number of international fora have attempted to address the jurisdictional challenges posed by cybercrime. The most extensive is the Council of Europe’s Convention on Cybercrime (CoE Convention), which was opened for signature on November 8, 2001, and has been signed by 33 countries. The CoE Convention addresses many of these issues. It creates a minimum list of cybercrime offenses and attempts to harmonize the elements of those offenses, thereby reducing many conflict-of-law and dual criminality issues. The CoE Convention requires signatories to establish criminal jurisdiction over offenses committed in their territory and to consult on investigations. When more than one signatory claims jurisdiction over an offense, they must consult to determine the most appropriate jurisdiction for prosecution. The CoE Convention makes all cybercrimes extraditable offenses and helps resolve extradition treaty conflicts between two signatory
countries. The CoE Convention requires signatories to provide mutual assistance “to the widest extent possible” in the collection and preservation of requested data, whether real-time or stored.

The G-8 has also taken steps to facilitate mutual assistance and resolve many of the jurisdictional issues associated with cybercrime. Likewise, the EU has launched several initiatives aimed at addressing these matters within the jurisdiction of its Member States.

D. LAW ENFORCEMENT

The rapid escalation of cybercrime has significantly affected law enforcement’s ability to investigate and prosecute crimes. In addition to coping with the technological advances associated with cybercrime, law enforcement increasingly has to deal with the role of cyber evidence and ICTs in traditional crimes such as murder, rape, illegal drug sales, and child pornography. Cybercrimes present law enforcement with three main challenges:

1. Technical challenges that are caused by (a) rapid changes in technology and the inability of law enforcement to stay current, and (b) technical shortcomings that impair finding and prosecuting cyber criminals.

2. Legal challenges that are caused by procedural barriers or hurdles and the inability of legal frameworks around the globe to keep up with technological capabilities and the changing business environment.

3. Operational challenges that are caused by (a) a lack of equipment, training, and adequate organizational structures, and (b) the need to work with great speed despite time zone, language, and cultural differences.

To address these challenges, governments must devote ongoing government attention and resources to training personnel in high-tech investigative and forensic techniques, establishing internal organizations, and actively participating on the international front. Combating cybercrime also calls for a new partnership between the public and private sectors to enable law enforcement to meet the challenges of high-tech crime. Such partnerships should be based on information sharing, cooperation, and joint work toward fostering global minimum standards.

The two overarching concerns common to all law enforcement agencies are time sensitivity and resource constraints. There is a grave risk that the ability to keep pace with cyber criminals will be outpaced
by advancements in technology. Law enforcement’s response must be swift, lest the criminals gain the upper hand. Existing resources must be spent wisely. A centralized, coordinated approach is needed when allocating resources to technical tools, training, on-site assistance, and research. The greatest impact is achieved when this is done through existing structures that have a broad reach and include most key stakeholders.

Ten critical priority needs that can be addressed at the national level to improve law enforcement’s ability to combat cybercrime are:

1. Increase public awareness of the incidence and impact of cybercrimes.
2. Improve data collection, analysis, and reporting on cybercrimes.
3. Establish uniform training and certification courses.
4. Establish electronic crime task forces with regional or national capabilities.
5. Bring legal frameworks up to date with technology and international laws.
6. Create better cooperation with the high-tech industry.
7. Establish a central repository and resource point for cybercrime materials.
8. Improve senior management’s understanding of cybercrime trends and needs.
9. Obtain up-to-date investigative and forensic tools.
10. Follow best practices when establishing electronic crime units.

The U.S. government’s activities in cybercrime are considered a worthy model by many countries. Numerous multinational organizations are addressing cybercrime, with the CoE, G-8, and UN in leadership roles. The CoE Convention is the first multilateral treaty that addresses many of the legal and procedural barriers and hurdles confronted by law enforcement and prosecutors in dealing with cybercrimes. It requires signatories to cooperate and offer timely legal assistance in the collection and preservation of evidence and in the investigation and prosecution of electronic crimes. In the past two years, the EU has also launched a number of cybercrime initiatives that are certain to have a global impact. The EU is currently considering a draft proposal for a Council Framework Decision on attacks against information systems that would help facilitate cooperation with law enforcement and address many of the ten priority areas listed above.

Despite these efforts, however, international activities lack coordination, and law enforcement continues to face barriers and procedural delays caused by inadequacies in legal systems and the lack
of a global, harmonized legal framework. Industrialized nations and donor organizations can advance this process by helping developing countries enact cybercrime laws, establish needed government entities, and provide critical training. The private sector can also help through assistance provided by the legal community, communication providers, private sector companies, and nongovernmental organizations (NGOs).

E. SEARCH AND SEIZURE

Absent consent or access to public communications, government interceptions of communications (and traffic data), and government seizures or compelled disclosures of data in the hands of businesses and individuals constitute an intrusion on personal privacy. Nearly every country in the world includes a right of privacy in its Constitution or other basic law. These provisions normally include rights of inviolability of the home and secrecy of communications. The right to privacy is also widely recognized as a fundamental human right under various human rights instruments, including the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the European Convention on Human Rights, and the American Convention on Human Rights. The provisions of the European Convention on Human Rights are binding on all 44 Member States belonging to the Council of Europe. The CoE Convention explicitly requires that searches and seizures be conducted pursuant to the principles set forth in the European Convention on Human Rights.

Under most legal systems, such search and seizure intrusions are permissible, but only in accordance with clear standards in the law, requiring justification and prior independent approval, often by a judge. Legal standards limiting the circumstances and procedures for interception, search, and seizure are evolving, but governments and international human rights bodies are paying increasing attention to the procedures.

Varying legal frameworks around the globe significantly complicate the search and seizure of electronic evidence. Distinctions are made between real-time interceptions and digitally stored evidence. For real-time interceptions, the laws in several countries distinguish between the interception of the content of communications and the interception of only the transactional data, or traffic data, that indicates the origin and destination of communications. Under almost all legal systems, the interception of communications is considered a privacy intrusion of the highest order, requiring strict legal protections.

Stored digital evidence can be obtained through immediate access to stored data by entry into a home or office. Under most legal systems,
this is considered a serious intrusion on privacy and requires prior legal approval, often by a judicial officer upon a showing by investigators of need and justification. Disclosure of stored data can also be compelled via a subpoena. These disclosures also intrude upon privacy interests and usually require some form of independent approval and oversight.

Law enforcement officials will increasingly be collecting electronic evidence, not only in cybercrime cases, but also in investigations of other kinds of crime that are facilitated by computers or involve electronic communications. This will require attention to both the practical and legal issues involved in accessing communications and stored data.

Developing nations seeking to update their criminal laws for the digital age should address the procedural standards for government access to communications and computer data, while balancing the protection of public safety with protection of privacy and civil liberties. They will also need to ensure that their investigators are adequately trained in the practical considerations surrounding the acquisition and analysis of digital evidence. The emerging body of international experience provides useful guidance and suitable models for both the legal and practical aspects of the search and seizure of digital evidence.

**F. PUBLIC/PRIVATE COOPERATION**

The security of networks and computers is part of the academic discipline of computer science, and the lack of security of networks and host computers is an important issue for everyone who uses the Internet. Security breaches, therefore, cannot be handled only by governments and law enforcement. The nature of cybercrime requires close cooperation between the public and private sectors. Electronic crimes can be committed by disgruntled or former employees, hackers and “script kiddies,” organized crime, domestic and foreign competitors, terrorists, and other nation states. The networks and systems under attack or used in cybercrimes are often operated by private companies. Whether and how a company responds to these attacks often involve a delicate evaluative balance among the potential financial losses or damage caused and the risks (legal, regulatory, and to business reputation) involved in reporting or failing to report such attacks, including potential lawsuits and/or third-party liability.

Public/private cooperation on cyber attacks and cyber criminal activities is important and helps each side better understand how to respond to cybercrime and mitigate its impact. This necessarily involves information sharing, which can mean different things to different
people. For some, it is a way to develop or enhance information security ideas cooperatively, collaborate on joint responses, or share resources for detecting, preventing, and responding to security breaches and criminal activities. For others, it can mean divulging competitively sensitive information or proprietary data, essentially giving the government—and potentially their competition—the “keys to their kingdom.” Some security researchers and professionals believe that information about security vulnerabilities, whether in networks or in host computers, should not merely be shared within industry or with government, but with academia and the general public as well. In whatever form information sharing takes, trust forms the critical element that facilitates the public/private cooperation necessary for the effective prevention and prosecution of cybercrime.

Neither government nor the private sector can address these problems standing alone. Governments cannot solve the complex and multilayered problem of cyber security and critical infrastructure protection without the assistance of private organizations. The government needs a cooperative relationship with the private sector because, in most instances, the government does not own, control, or operate the networks that underpin most critical sectors. The private sector needs the government because, no matter how large the corporation, it cannot by itself defend against attacks from terrorists or economic espionage from nation states. Moreover, the core of any nation state’s economy, national security, and public safety is dependent upon the reliability, integrity, and availability of its critical infrastructures: electric power grids, railroad and airlines, oil and gas, banking and financial systems, and communications networks. Each of these is dependent upon ICTs and the global, interconnected network.

The legal frameworks of countries often discourage information sharing because they do not provide adequate protections from disclosure of shared information under freedom of information, antitrust, and privacy laws and other potential liabilities related to disclosure of the information. Information sharing and analysis centers (ISACs), which have been voluntarily formed by private sector members, have been cited around the world as models for cooperation and information sharing between the public and private sectors. The common benefits to ISAC members are early notification of potential cyber risks; access to relevant information; industry-wide vigilance; increased subject matter expertise; and access to trending, metrics, and benchmark data.

Information sharing can be facilitated by public sector initiatives that (a) establish centers for sharing information on an anonymous
basis or serve as an intermediary where the direct sharing of information among industry is difficult, (b) create a central alert point for technical information and assistance regarding security risks and fixes, and (c) organize a public/private group comprised of all stakeholders (industry, government, academia, NGOs) to begin a dialogue on ICT security risks and develop ways to work together. Activities by private sector entities, such as the insurance, auditing, and high-tech industry sectors, can also advance information sharing and increase information and infrastructure security.

Numerous initiatives are under way on the international front, but there remains a general lack of coordination and harmonization of legal frameworks that, in the end, impedes efforts to combat cybercrime.
Introduction

A. BACKGROUND

With nearly 200 countries connected to the Internet, cybercrime has become a global issue that requires the full participation and cooperation of the public and private sectors in all countries, including the 180 developing countries around the globe. A major component of information and infrastructure security is a nation’s ability to deter, detect, investigate, and prosecute cyber criminal activities. Weaknesses in any of these areas can compromise security not only in that country, but around the globe. This is because of the global, interconnected nature of the Internet and the way in which countries must rely upon each other’s expertise and assistance in addressing cybercrime matters. Therefore, industrialized and developing countries must approach cybercrime in a coordinated fashion. It is not enough that the Group of Eight (G-8) countries\(^1\) have worked together to counter cybercrime or that the Council of Europe (CoE) has adopted a *Convention on Cybercrime* that has been signed by 33 countries. *Every* country must address cybercrime lest it becomes the weakest link in global cyber security.

The glaring gaps in work to date are (1) inadequate international coordination and (2) woefully deficient legal frameworks and organizational capacity in developing countries necessary to combat cybercrime. The ABA’s International Cybercrime Project\(^2\) was designed

---

\(^1\)The G-8 countries are the United States, Canada, United Kingdom, France, Germany, Italy, Japan, and Russia.

\(^2\)The International Cybercrime Project is an activity of the American Bar Association’s Section of Science & Technology Law, Privacy and Computer Crime Committee.
to bring together ABA members and key stakeholders from government, industry, nongovernmental organizations (NGOs), and academia to address issues in five areas important to combating cybercrime. The *International Guide to Combating Cybercrime* is intended to serve as a manual for developed and developing countries alike to help them (1) create effective cybercrime laws, (2) handle jurisdictional issues, (3) cooperate in international investigations, (4) develop acceptable practices for the search and seizure of electronic evidence, and (5) establish effective public/private sector interaction.\(^3\)

By explaining the importance of these issues, the ABA Privacy and Computer Crime Committee believes this project will:

- Help developing countries attract foreign direct investment and offshore technology operations, and bring the economic and social benefits of technology to their people.
- Promote international cooperation and coordination in combating cybercrime and encourage the establishment of public and private sector structures necessary to share resources and effectively deal with these issues.
- Help government officials, industry, citizens, academia, and nongovernmental organizations understand their role in combating cybercrime.

### B. ACTIONS BY THE GROUP OF EIGHT AND COUNCIL OF EUROPE

Cybercrime poses one of the biggest threats to the widespread deployment and utilization of information and communication technologies (ICTs) around the globe. Whether in the form of hacking, economic espionage, web defacement, sabotage of data, viruses, fraud, unauthorized access to or disclosure of data, or other acts against computers, networks, and data, cybercrime affects everyone—businesses, governments, and citizens. Struggling to keep pace with technological developments, industrialized countries have been individually addressing cybercrime issues for several years. By 1997, they realized that the borderless world of the Internet, the international

---

\(^3\)The views expressed herein have not been approved by the Council of the Section of Science & Technology Law, the House of Delegates, or the Board of Governors of the American Bar Association. Nor do the views expressed herein reflect the views of the organizations to which Project participants outside the ABA belong.
nature of packet switching, and a lack of cooperation and assistance between communication providers and law enforcement around the globe required a more coordinated approach.

1. G-8 Initiatives

In December 1997, the G-8 Meeting of Justice and Interior Ministers responded to increased international movement and use of ICTs by organized crime, other criminals, and terrorists. The ministers noted:

National laws apply to the Internet and other global networks. But while the enactment and enforcement of criminal laws have been, and remain, a national responsibility, the nature of modern communications networks makes it impossible for any country acting alone to address this emerging high-tech crime problem. A common approach addressing the unique, borderless nature of global networks is needed and must have several distinct components.

Each country must have in place domestic laws that ensure that the improper use of computer networks is appropriately criminalized and that evidence of high-tech crimes can be preserved and collected in a timely fashion. Countries must also ensure that a sufficient number of technically literate, appropriately equipped personnel are available to address high-tech crimes.

Such domestic efforts must be complemented by a new level of international cooperation since global networks facilitate the Commission of transborder offenses. Therefore, consistent with the principles of sovereignty and the protection of human rights, democratic freedoms and privacy, nations must be able to collect and exchange information internationally, especially within the short time frame so often required when investigating international high-tech crimes.4

Subsequently, the heads of the G-8 nations endorsed the ministers’ ten Principles to Combat High-Tech Crime and Action Plan to Combat High-Tech Crime.5 A G-8 24/7 Point of Contact Network was then established, requiring countries to designate a 24-hours-per-day,

---

7-days-per-week Point of Contact to provide assistance with crimes involving electronic evidence. Approximately 30 countries are currently participating in the program. Additionally, a G-8 high-tech experts group was formed to improve mechanisms for locating and identifying cyber criminals and to address issues such as data preservation, tracing, user authentication, and international cooperation.

More recently, at the July 2000 Okinawa Summit, the G-8 strongly endorsed international cooperation and coordination regarding cybercrime by declaring in the Okinawa Charter on Global Information Society:

International efforts to develop a global information society must be accompanied by coordinated action to foster a crime-free and secure cyberspace. We must ensure that effective measures, as set out in the OECD Guidelines for Security of Information Systems, are put in place to fight cyber-crime. Urgent security issues such as hacking and viruses also require effective policy responses. We will continue to engage industry and other stakeholders to protect critical information infrastructures.

With only a few exceptions, however, the work of the G-8 has not been extended to the 180 developing countries around the globe.

2. Council of Europe Cybercrime Convention

After four years of work, the Council of Europe’s 44 Member States and partner countries (Canada, Japan, South Africa, and the United States) recently completed the first binding, multilateral treaty on cybercrime. On November 8, 2001, the CoE’s Committee of the Ministers adopted a Convention on Cybercrime (CoE Convention), which, to date, has been signed by 29 member countries, plus the four partner countries. The primary goal of the Convention, as noted in the preamble, is to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia by adopting appropriate legislation and fostering international cooperation. The treaty becomes effective upon ratification by five

---

8CoE Convention, Preamble.
countries, three of which must be CoE Member States. Other nonmember states may be invited by the CoE’s Committee of Ministers to sign the Convention.

C. THE OPPORTUNITY FOR DEVELOPING COUNTRIES

ICTs bring both opportunities and challenges to developing countries. The G-8, World Bank, UN, and U.S. Agency for International Development (USAID) are each committed to bridging the global “Digital Divide.”9 The donor community10 also understands that ICTs are a powerful development tool that can help boost economies, increase competitiveness, attract foreign direct investment (FDI), and raise the skill level of the workforce in developing countries. Developing countries also realize the potential impact of technology, and many are launching their own ICT initiatives and aggressively competing for donor funds to assist them.

Internet growth works in their favor. Today, there are approximately 600 million people connected to the Internet. However, that online population accounts for only 10 percent of a world population of about 6 billion people. With 65 percent of Americans already online,11 in the future we can expect some of the highest connectivity increases to be in the 180 developing countries around the globe. Indeed, Forrester Research predicts that by 2007, 70 percent of software programming will be performed in developing countries.12

Thus, developing countries have an unprecedented opportunity to seize upon the advantages of ICTs to propel their progression toward industrialization, market economies, and social advancements. These opportunities include:

- Attracting foreign direct investment to (a) build infrastructure, (b) launch ICT projects, (c) partner with donor organizations and governments on pilot projects, and (d) tap undeveloped markets.

---

10The donor community consists of aid institutions such as The World Bank Group, the U.S. Agency for International Development (USAID), United Nations (UN), Canada International Development Agency (CIDA), European bank of Reconstruction and Development (EBRD), Inter-American Development Bank (IADB), and numerous other development banks and assistance organizations.
Privatizing and liberalizing monopoly providers to introduce competition, lower prices, and advance the deployment and utilization of ICTs.

- Attracting data processing applications such as data entry, customer service and telemarketing operations, records processing (accounts receivable, accounts payable, general ledger, and so forth), order entry, inventory control, databank development, data storage operations, remote systems administration, and the like.
- Attracting Internet start-up companies, e-commerce operations, and software development centers.
- Developing telemedicine and health care centers.
- Using ICTs for distance learning, education, unemployment databases, and workforce skills.
- Using ICTs for agribusiness and agricultural information and industry sector support.
- Attracting light manufacturing operations.
- Modernizing the financial sector.
- Fostering the growth of small and medium-sized enterprises (SMEs) to spur job creation, innovation, flexibility, and competitiveness.
- Reforming and automating court administration and case management and availability of judicial information.

Each of these opportunities, however, is dependent upon the development of the legal and regulatory framework to support them. The legal framework is one of the most important factors because it touches upon all aspects of commerce, is critical to attracting investment, and is at the core of providing certainty to business operations. The term “legal framework” also includes public policy, which forms the underlying foundation of government support for ICTs and a favorable business environment.

D. THE IMPORTANCE OF CYBERCRIME LAWS AND ICT SECURITY

The confidentiality, integrity, and availability of data and networks—including critical infrastructure—are central to attracting FDI and ICT operations to developing countries. The opportunities associated with ICTs are not guaranteed; they are dependent upon developing countries’ ability to effectively address the additional challenge of cyber security and to take steps to actively participate in the global community in combating cybercrime.
Appropriate security laws and regulations are also important because:

- They protect the integrity of the government and reputation of the country.
- They help preclude a country from becoming a haven for bad actors, such as terrorists, organized crime, and fraud operations.
- They help prevent a country from becoming a repository for cyber criminal data.
- They instill market confidence and certainty regarding business operations and attract foreign direct investment.
- They provide protection of classified, secret, confidential, and proprietary information, criminal justice data, personal information, and protected public data.
- They protect consumers and assist law enforcement and intelligence gathering activities.
- They deter corruption.
- They increase national security and reduce vulnerabilities from attacks and actions by terrorists and other rogue actors.
- They help protect corporations against risk of loss of market share, shareholder and class action lawsuits, damage to reputation, fraud, and civil and criminal fines and penalties.
- They provide a means of prosecution and civil action for acts against information and infrastructure.
- They increase the chance that electronic evidence in physical-world crimes, such as murder or kidnapping, will be available when needed.

Security and cybercrime laws are important to citizens because they help reinforce and protect their freedom of expression, human rights, and other legal rights that are secured in international law. Cybercrime laws enhance statutory and constitutional rights, such as rights to privacy and protections against search and seizure and self-incrimination. They help ensure that citizens can access information, exchange information, and protect the privacy of their personal, confidential, and proprietary information. Additionally, they strengthen consumer confidence against fraud.

For the most part, developing countries are struggling with how to use e-commerce and ICTs in everyday government and business operations. Most have not begun to even address cybercrime and have weak or no cybercrime laws. With the exception of a few small initiatives, donor organization work has focused on telecommunications liberalization and the framework needed to support e-commerce, not
on cybercrime issues. Therefore, developing countries frequently become the weakest link in cyber security.

The lack of an adequate legal framework—especially with respect to information and infrastructure security and computer crime—will diminish or prevent developing countries from grasping ICT opportunities. The reasons are clear:

- Internet and e-commerce operations require an enabling legal framework that also provides for security of data and networks.
- Data processing operations require information and infrastructure security laws for a safe operating environment and protection of data.
- Companies will not allow their data to be processed in countries that do not have adequate legal protections against economic espionage, computer crime, infrastructure attacks, and misuse of telecommunications devices and equipment.
- Certain laws, such as the EU data protection directive, require that countries afford equal legal protections against misuse of personal data.

E. INTERNATIONAL COOPERATION NEEDED FOR GLOBAL CYBERCRIME PROBLEMS

International coordination and cooperation are as significant as the legal and regulatory framework. Cybercrime laws accomplish little without the internal government structures and skilled personnel that are necessary to effectively deal with jurisdictional issues, international requests for assistance, and the search and seizure of electronic evidence.

Cybercrime presents one of the most complex and pressing circumstances for international cooperation. The U.S. President’s Working Group on Unlawful Conduct on the Internet noted that, “Inadequate regimes for international legal assistance and extradition can . . . in effect, shield criminals from law enforcement: criminals can go unpunished in one country, while they thwart the efforts of other countries to protect their citizens.”13 While nation states still have physical borders, cyber space does not and jurisdictional issues loom over numerous e-commerce issues. A country must possess the legal

---

authority to assist foreign countries in an investigation, even if the country at issue has not suffered any damage but is merely the location of the intruder or a pass-through site.

Cyber criminals do not have to leave their own homes—or cross a national boundary—to commit an act in several countries around the globe. Their communications may be routed through local phone companies, long-distance carriers, Internet Service Providers (ISPs), and wireless and satellite networks, and they may go through computers located in several countries before attacking targeted systems around the globe. Someone can commit a cybercrime, such as fraud, against persons in several countries simultaneously and with anonymity. Evidence of the cybercrime may even be stored on a computer in a different country from where the criminal executed the act. Foreign assistance also may be needed even if the act is local. Frequently, communications may pass through several countries, requiring law enforcement to seek international assistance just to find out the perpetrator is a local person. For example, an e-mail sent to a colleague across town may be routed via packet switching through countries on three continents before reaching the recipient’s inbox.

Clearly, a coordinated and consistent approach to foreign country assistance in the investigation and prosecution of cybercrimes is needed in order to deal with trails of electronic communications scattered across different time zones and multiple jurisdictions with differing legal systems and levels of technical skills. Around-the-clock assistance regarding cybercrimes is necessary because investigation of a single communication may require multiple court orders and legal assistance from several countries—when time is of the essence. In sum, global cyber security is dependent upon developing countries having effective legal and regulatory frameworks, skilled and cooperative law enforcement, 24/7 availability of key personnel, and accepted principles for search and seizure of computers and data.

F. SCOPE OF INTERNATIONAL CYBERCRIME PROJECT

The ABA International Cybercrime Project will (a) promote international cooperation and coordination on combating cybercrime and (b) extend the work of the G-8, Council of Europe, and other multinational organizations and industrialized nations regarding cybercrime to developing countries with the goal of promoting:

- Enactment of cybercrime laws and development of a harmonized legal framework.
Respect for human rights, privacy, and safety.
- Cooperation on and resolution of jurisdictional issues.
- Cooperation among law enforcement, communication providers, and e-commerce companies.
- Acceptable practices for search and seizure of computers and electronic data that are effective yet balanced.
- Cooperation between public and private sector entities on combating cybercrime.

By explaining the importance of these issues to their future development, the ABA Privacy and Computer Crime Committee believes this project will help developing countries attract FDI and offshore ICT operations and bring the economic and social benefits of technology to their people.

This Guide is designed as a cybercrime manual that includes a chapter devoted to each of the main problems identified above, which are encountered by all countries in combating cybercrime:

- **Chapter 1** discusses key cybercrime laws and sets forth a compilation of laws from the United States, Canada, Europe, and Asia (to the extent they are available), with a summary of each and links or cited references to the statutes. This chapter also includes guidance on the need for balanced and fair cybercrime laws that respect international human rights, freedom of expression, and privacy.
- **Chapter 2** discusses the jurisdictional issues related to the detection and investigation of cybercrime and what a country can do to minimize jurisdictional problems.
- **Chapter 3** serves as a guide to cooperating with national and international law enforcement, communication providers, and ISPs.
- **Chapter 4** discusses acceptable practices for search and seizure of computers and electronic data, with links to U.S. and international search and seizure guides.
- **Chapter 5** discusses the critical role played by public/private sector interaction in combating cybercrime and serves as a guide to establishing effective cooperation on these issues.

This Guide was written as a cooperative effort between members of the ABA Section of Science & Technology Law’s Privacy & Computer Crime Committee and interested personnel from outside organizations that actively participated in and contributed to the process. All in all, the project proceeded with the involvement of all stakeholders—lawyers, privacy and consumer advocates, academia, industry, and government.
CHAPTER ❖ 1

Cybercrime Laws

I. Introduction
A. BACKGROUND

Countries looking to encourage domestic and international confidence, development, and investment have established legal regimes that protect critical information networks, information systems, and digital data. Today these laws work to protect more than just computers and databases; they help secure facilities, people, and information and communication systems. Consider that advanced building security systems usually restrict access by requiring the insertion of a magnetic or encoded card into a reader that is controlled by a computer system. Manufacturing processes—from robotic assembly and delivery of parts on assembly lines to flows of gases and chemicals and control of complex processes—are all managed by ICT systems. Employees and executives alike depend upon technology to perform their jobs and rely upon cell phones, Personal Digital Assistants, and pagers to manage their communications, calendars, appointments, and contact information. Data is no longer kept only in hard copy; at least 80 percent of corporate intellectual property is digital.¹

No matter where ICT systems are—in a developing or highly industrialized country—they can be compromised for a number of reasons: (a) to allow access to unauthorized persons into a facility, (b) to enable someone to steal or sabotage data, (c) to manipulate

design-process systems and critical infrastructure to cause a catastrophic event, or (d) to intercept data and communications. Infrastructure attacks can also take a variety of forms. One of the more common is the distributed-denial-of-service attack (DDOS). These attacks are launched from tens or hundreds of computers around the world. Prior to the attack, hackers break into computer workstations and servers with high-speed Internet connections and install hard-to-detect malicious software. At the designated time, a signal is sent via the Internet to these computers to launch the hidden programs, causing the targeted site to be flooded with bogus requests for information to the point the site can become jammed.2

In approaching legal and policy considerations regarding cybercrime, it is also helpful to have a layperson’s understanding of malicious software, commonly called “malware,” and the categories of security threats. Brief descriptions are offered here; a wealth of information regarding security risks is available on the Internet.3

**Virus.** A virus is a program that is intentionally written and launched. Viruses’ most common traits are their ability to (1) attach themselves to a host program and run when the host is run and (2) replicate themselves. Their authors intend them to run inside a computer and impact the data or integrity of the computer without the owner’s knowledge. Today there are over 50,000 known viruses, and experts estimate an additional 1,000 are created every month. They can spread through infected floppy disks and e-mail attachments and be downloaded as part of a larger file from a network or the Internet. There are various types of viruses, but they should all be considered harmful.4 The 2002 CSI/FBI Computer Crime and Security Survey reported that the global economic impact of the Code Red virus was

---

US$2.62 billion. The less recent I LOVE YOU virus and its variants infected tens of millions of users and caused an estimated US$8.75 billion in economic damages.\(^5\)

**Trojan Horse Programs.** Trojans, unlike viruses, do not replicate. They hide inside another program and when that program runs, the Trojan is launched and performs undesirable actions to the system and/or data.

**Worms.** Worms replicate, not infect. They can use a network to copy themselves onto other machines. A worm can separate into pieces across a network or replicate itself many times on a hard drive. They can be spread through e-mail or Internet relay chat.

**Bombs and Droppers.** Bombs are pieces of software that activate a malicious program, such as a virus. Droppers are programs that transport and install viruses.\(^6\)

**Web-Jacking.** Web-jacking results in the manipulation of websites and search engines to send unsuspecting users to other sites, usually adult or pornographic sites.\(^7\)

**Steganography.** Steganography is often accomplished by using a software program to hide data, pictures, or text within another document or image, where it is invisible to the eye and undetected by firewalls. Special software is needed to detect data hidden by steganography.

The foregoing list shows that the Internet, networks, and e-mail—three important uses of technology in developing countries and central to e-commerce—are the most common means of spreading viruses and malicious software because the link to outside networks creates a portal for hackers.\(^8\) If for no other reason, security must be a priority to


\(^6\)Dr. Dorothy E. Denning, Georgetown University, Testimony before Special Oversight Panel on Terrorism, Committee of Armed Services, U.S. House of Representatives, May 23, 2000, at 16.


prevent destructive malware from interrupting or damaging systems and data.

Cybercrime laws deter cyber criminal activities and make these offenses punishable, but they vary in form as much as cybercrime itself. Industrialized nations have enacted laws protecting computer and communications systems and the data residing in and transiting these systems. Generally, these cybercrime laws apply to:

- Use of computers and the Internet for illegal purposes (viruses, hacking, unauthorized access).
- Crimes against communication systems.
- Crimes facilitated by the use of a computer.
- Wiretap, pen register, and trap-and-trace laws to protect privacy and facilitate investigations.

Industrialized countries have also updated their criminal codes to ensure statutes can be applied by diligent law enforcement authorities and government prosecutors to traditional crimes committed in new ways through computers and the Internet. Nations at the forefront of retooling their criminal legal systems to combat cybercrime have also supplemented these efforts with additional laws and policies promoting electronic authentication and the use of encryption and relaxing controls for import and export of encryption devices and software.

One of the challenges countries face is keeping their computer crime laws up to date. Cybercrime laws are constantly evolving with new technological capabilities and criminal innovation to address new forms of computer crime, new types of criminals, and emerging concerns within the law enforcement community. Several trends are evident.

First, in response to the terrorist attacks of September 11, 2001, and the cybercrime concerns arising out of it, the United States and Australia have modified their respective computer crime laws so that they cover unlawful access to government, law enforcement, and national security computers.

Second, with improvements in telecommunications and computer technology throughout the world, making computer crime a seemingly borderless crime, crimes by and against foreign computer systems have proliferated. Nations have responded to transborder cybercrime by modifying their criminal codes to allow for jurisdiction over, and prosecution of, individuals and organizations committing crimes from one country against computers located in another.

Finally, seeking to demonstrate integrity of their computing and information infrastructures and responsiveness to the accelerating concerns of industrialized nations as expressed through the Organization for Economic Cooperation and Development (OECD),
the Financial Action Task Force (FATF), and the Bank for International Settlements (BIS), developing nations have increasingly adopted and improved their computer crime laws to emulate the laws of more developed nations.

Modeling cybercrime laws after those put forth by multinational organizations and countries that are leaders in commerce is the correct approach. Developing countries should take a global perspective when creating a legal and regulatory framework regarding ICTs. They are encouraged to participate in UN activities in this regard, to join multinational organizations, and to become global players as these issues are discussed and debated and new global legal structures are formed. Countries in line for accession into the European Union, of course, should closely monitor EU developments in the cybercrime arena. Likewise, countries in the Asia-Pacific region should be mindful of directions from the Asia-Pacific Economic Cooperation forum. The leading multinational organizations involved in the ICT legal arena are the UN, OECD, World Trade Organization (WTO), EU, CoE, and APEC. Although not a multinational entity, the United States is also influential regarding ICT legal/regulatory issues.

As the global legal and regulatory framework develops for e-commerce and security issues, it is generally accepted that online conduct be treated no differently than offline conduct. In other words, laws should be technologically neutral and based upon the act rather than the technology used to commit the act. As former FBI Director Louis Freeh noted in testimony before the U.S. Senate, “Statutes need to be rendered technology neutral so that they can be applied regardless of whether a crime is committed with pen and paper, e-mail, telephone, or geosynchronous orbit personal communication devices.”[9] Along the same lines, many existing laws are out of step with technological advances and need to be repealed or updated to accommodate the online world.

B. CHAPTER OVERVIEW

The laws summarized in this chapter offer guidance for countries looking to introduce or develop effective cybercrime laws. This chapter provides a summary of the current law in this area and provides linking information to sites having up-to-date statutory and regulatory information and material. Part II covers national legal regimes

addressing crimes against computer systems, Part III covers crimes against communication systems, and Part IV covers crimes facilitated by computers and the Internet. Part V covers supplementary laws promoting electronic transactions, digital signatures, message authentication, and data security.

II. Laws on Crimes against Computer Systems

A. INTRODUCTION

Many countries have laws concerning crimes against computers. By recognizing that the first step in cybercrime is access to and use of computers by criminals, hackers, and malicious parties, nations have enacted computer crime laws that have several common elements:

- The laws make it a criminal offense to obtain access without the owner’s authorization to a computer system (for example, any computer connected to a network) or, as in some laws, to a protected class of computer systems (such as financial computer systems or government systems); and
- The laws criminalize certain acts following computer access, such as (a) unauthorized access to data or the modification or destruction of data or software residing in a computer system and (b) the unauthorized use of computer time and resources.

Developing countries must enact laws that criminalize the use of computers, access devices, and the Internet for criminal purposes. There is no better example to date than the Philippines’s inability to prosecute the author of the I LOVE YOU virus because it did not have a law that made his conduct illegal. Although a law was passed shortly after the incident occurred, it could not be applied retroactively. This incident damaged the Philippines’s credibility as a viable site for e-commerce and ICT activities. A similar incident in Romania resulted in the author of a virus not being prosecuted for lack of an applicable law, tainting the country as a hotbed for viruses.

B. NORTH AMERICA—LAWS ON CRIMES AGAINST COMPUTER CONTENT AND SYSTEMS

1. United States

In the United States, the most significant computer crime law is the Computer Fraud and Abuse Act (CFAA).\(^\text{10}\) In response to the terrorist acts

\(^\text{10}\)18 U.S.C. Section 1030 et seq.; the text of the Computer Fraud and Abuse Act can be found at http://www.usdoj.gov/criminal/cybercrime/1030_new.html.
of September 11, 2001, and the accompanying cybercrime concerns, portions of the CFAA were amended by the U.S. Congress through its passage of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act of 2001). The CFAA, as amended, covers computer fraud and related activity against or involving a computer that is protected. A "protected computer" under the CFAA is a computer or computer system that is used by (1) a financial institution, (2) the U.S. government, or (3) one that is used in communications or commerce between the states of the United States (known as interstate commerce) or foreign commerce, including foreign computers that affect U.S. communications or foreign or interstate commerce.

Under the CFAA, it is a crime to:

1. Access a computer without authorization or to exceed authorization and, by doing so, access classified information pertaining to foreign relations or national defense.

2. Access a computer, either without authorization or by exceeding authorization, and obtain (a) information pertaining to financial institutions or credit agencies, (b) information from a U.S. government department or agency, or (c) information from a protected computer if the conduct involved an interstate or foreign communication.

3. Intentionally access without authorization (a) any nonpublic computer of the U.S. government or (b) any computer that is not exclusively used by a U.S. government department or agency but is accessed in order to affect its use by the government.

4. Access a protected computer without authorization and knowingly and intentionally commit fraud that is valued at US$5,000 or more for a one-year period.

5. (i) Transmit or attempt to transmit a program, information, code, or command without authorization that intentionally causes damage to a protected computer; (ii) intentionally access or attempt to access a protected computer without authorization and recklessly cause damage; or (iii) intentionally access or attempt to access a protected computer without authorization and cause damage. In these circumstances, damages are the aggregate loss of at least US$5,000 in a one-year period, which considers the value of the actual damages caused by the

---

Authorized transmission or access (or in the case of an attempted offense, the damages that would have been incurred if the act had been completed) plus the costs of restoring the system and other foreseeable damages.\textsuperscript{12} The damages threshold is not required if the act (a) caused or intended to cause a modification or impairment of medical records or treatment information; (b) caused or would have caused a threat to public health or safety; or (c) caused or would have caused damage to a government computer used in the administration of justice, national defense, or national security.

6. Traffic in passwords or other information that may be used to gain unauthorized access to protected computers, if such trafficking affects interstate or foreign commerce or the computer in question is used by the U.S. government.

7. Transmit a communication that threatens to cause damage to a protected computer in an attempt to extort payment or something of value.

Acts within the scope of the CFAA are criminal offenses and are punishable by a fine or imprisonment, or both, and apply to both offenses and attempted offenses.

For offense 1 above, a fine and term of imprisonment of not more than ten years, or both, apply if the offender had not previously been convicted for another offense under the CFAA. If the offender had previously been convicted under any part of the CFAA, he/she would be subject to a fine and not more than twenty years of imprisonment, or both.

For offenses 2, 3, 5(iii), and 6 above, fines and imprisonment, or both, apply as follows:

- A fine and not more than a one-year term of imprisonment, or both, may apply if the offender was not previously convicted for an offense under the CFAA. For offense 2, this sentence applies only if the act or attempted act was (a) not committed for purposes of commercial or private financial gain, (b) not committed in furtherance of a criminal or tortious act in violation of U.S. laws or Constitution, or (c) the value of the information was US$5,000 or less.

\textsuperscript{12}This language incorporates the court’s holding in \textit{United States v. Middleton}, 231 F.2d 1207, 1210–11 (9th Cir. 2000) (damages under CFAA may be calculated based on salaries paid to, and hours worked by, in-house employees who repaired the damage done by an unauthorized intruder as well as other natural and foreseeable damages).
- A fine and not more than a five-year term of imprisonment, or both, apply for offense 2 if the offense or attempted offense (a) was committed for purposes of commercial advantage or private financial gain, (b) was committed in furtherance of a criminal or tortious act in violation of U.S. laws or Constitution, or (c) the value of the information obtained exceeds US$5,000.

For offenses 2, 3, and 6 above, the offender is subject to a fine and imprisonment of not more than ten years if the offender has previously been convicted of any offense under the CFAA.

For offenses 4 and 7 above, a fine or not more than a five-year term of imprisonment, or both, apply if the offender has not previously been convicted for any offense under the CFAA.

For offenses 4, 5(iii), and 7 above, a fine or not more than a ten-year term of imprisonment, or both, apply if the offender has been previously convicted of any offense under the CFAA.

For offense 5(i) above, a fine or not more than ten years’ imprisonment, or both, apply.

For offense 5(ii) above, a fine or not more than five years’ imprisonment, or both, apply.

For offenses 5(i) and 5(ii) above, a fine or not more than twenty years’ imprisonment, or both, apply if the offender has been previously convicted of any offense under the CFAA.

U.S. law also protects the equipment and lines of communications providers. This covers communication lines, stations, or systems and imposes criminal penalties for any attempt to willfully or maliciously injure or destroy any of the works, property, or material of any radio, telegraph, telephone or cable, line, station, or system, or other means of communication, operated or controlled by the government, or used for a military or civil defense function. This law is an important protection for communications infrastructure and is supplemented by recent efforts of the U.S. government to heighten awareness of, and strengthen industry and government responsiveness to, vulnerabilities in the nation’s critical infrastructure. In fact, the National Infrastructure Protection Center was established to serve as a focal point for threat assessment, warning, investigation, and response assistance to threats or attacks to critical information infrastructure, including

---

13 U.S.C. Section 1362. The text of this provision can be found at http://www4.law.cornell.edu/uscode/18/1362.html.
14 For more information on the National Infrastructure Protection Center, see http://www.nipc.gov/.
telecommunications networks, energy systems, banking and finance systems, water systems, government operations, and emergency services.

2. Canada

The key federal cybercrime provisions in Canada are sections 342.1 (Unauthorized Use of Computer)\(^{15}\) and 430(1.1) (Mischief in Relation to Data)\(^{16}\) of the Criminal Code of Canada (Criminal Code).

(i) Unauthorized Use of Computer
Section 342.1, often described as the “computer abuse” provision, protects the integrity of computers and computer-related communications. This section:

- Prohibits the theft of computer services by making it an offense to obtain “any computer service” fraudulently and without “colour of right” or authorization.
- Protects privacy by making it an offense to intercept “any function of a computer system.”
- Makes it an offense to use a computer system with the intent to commit the foregoing offenses.
- Targets persons who trade in computer passwords or who crack encryption programs by making it an offense to use, possess, or traffic in a computer password, or permit another person to have access to a password that would enable the commission of any of the foregoing offenses.

This provision is broad in scope, thanks in part to the expansive definition of “computer system,” which covers all computer systems and is not limited to a class or classes of protected computers. Those convicted of an offense under this provision of the Criminal Code are subject to imprisonment for a term not exceeding ten years.

(ii) Mischief in Relation to Data
The second relevant section is Section 430(1.1), which covers mischief to data and makes it an offense to:

- Destroy or alter data.
- Render data meaningless, useless, or ineffective.


\(^{16}\)Section 430(1.1) of the Criminal Code of Canada on Mischief in Relation to Data can be found at http://lois.justice.gc.ca/en/C-46/39560.html.
Laws on Crimes against Computer Systems

- Obstruct, interrupt, or interfere with the lawful use of data.
- Deny authorized persons access to data.

Data is defined in both sections of the code to include “representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer system.” Given the scope of the provision and the definition of “data,” the “Mischief to Data” section is broad enough to cover many typical types of computer attacks. It would, for example, extend to the release of a virus or the launch of a distributed denial of service attack. As written, however, the Criminal Code does not cover the mere possession of a virus program or a denial-of-service attack tool. The section currently comes into play only upon actual damage or interference. The possession of a virus program or denial of service tool could be captured, however, by Section 342.1,17 which, as noted above, makes it an offense to use a “computer system” with “intent” to commit an offense under this section. This is one of the areas Canada intends to clarify to comply with its obligations as a signatory of the Council of Europe Convention on Cybercrime. In order to constitute an offense within the reach of this section, the act must be committed “willfully.”18 Thus, this section would not extend to a person who, for example, simply forwards a virus with no intention to do so. Those convicted of an offense under this provision of the Criminal Code are subject to imprisonment for a term not exceeding five years.

C. EUROPE—LAWS ON CRIMES AGAINST COMPUTER SYSTEMS

1. United Kingdom

The current cybercrime legislation in force in England is the Computer Misuse Act of 1990 (CMA).19 Similar to Canada’s approach, the Act applies to all computer systems, deviating from the protected-computer-system approach in the U.S. Computer Fraud and Abuse Act. Under the CMA, it is an offense to intentionally gain unauthorized access to a computer system. It is also an offense to gain unauthorized access to a computer system with the intent to commit any offense.

18"Willfully" extends to both positive acts and omissions of acts when there is a legal duty to act.
The CMA is a criminal law, and convicted offenders are subject to imprisonment anywhere from six months to five years depending on the nature of the offense committed through unauthorized computer access—in addition to a range of criminal fines.

The CMA is notable for reaching beyond crimes against computer systems. It covers traditional offenses committed with the aid of or through unauthorized computer system access, and therefore encompasses such crimes as money laundering and child pornography. The CMA also covers the intentional impairment, modification, or destruction of computer programs or data stored on a computer. The United Kingdom was the first country to address the issue of extraterritorial jurisdiction for computer crimes (an area that was of some concern in the United States as well, hence the clarification of this issue in the USA PATRIOT Act amendments to the CFAA). From the onset, the United Kingdom has claimed jurisdiction over a party who gains unauthorized access to a computer that is in the United Kingdom, regardless of where the party in question may be located. Therefore, if someone in a foreign country was backhacking through computer systems in an attempt to determine the source of an attack on his or her computer system and backhacked into a U.K. computer, the person could be subject to the jurisdiction of U.K. courts and criminal penalties.

2. Council of Europe

On November 23, 2001, the Council of Europe (CoE) adopted its Convention on Cybercrime (CoE Convention or treaty). Once the treaty enters into force upon ratification by five signatory nations (three of which must be CoE members), then all signatories of the CoE Convention, including nonmember “partner states,” are required to harmonize their legal frameworks with the CoE Convention. The CoE Convention defines several activities, if committed with the necessary

---

20 Extra-territorial jurisdiction means that a country claims it has jurisdiction over persons or acts outside its national borders where such persons or acts commit or constitute crimes within its borders. This is usually justified because of the impact of the act on persons or entities within the borders of the country. The exercise of extra-territorial jurisdiction can raise international legal issues and disputes among nation states.


22 The non-member signatory nations include Canada, Japan, South Africa, and the United States.
intent, to be cybercrime offenses and makes them subject to criminal penalties:

- Intentional access without right to the whole or part of any computer system (the treaty does not contain the concept of a “protected” computer).
- Intentional interception, without right, of nonpublic transmissions of computer data.
- Intentional damage, deletion, deterioration, alteration, or suppression of computer data without right (parties can reserve the right to require that it causes serious harm).
- Intentional and serious hindering of the function of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data.
- The production, sale, procurement for use, importation, or distribution of devices designed to commit any of the above crimes, or of passwords or similar data used to access computer systems, with the intent of committing any of the above crimes.
- Intentional input, alteration, deletion, or suppression of computer data resulting in inauthentic data with the intent that such data be relied upon as if authentic.
- Intentional input, alteration, deletion, or suppression of computer data or any interference with the functioning of a computer system with the fraudulent intent of procuring an economic benefit for oneself.

Of additional note is the CoE Convention’s article on corporate liability (Article 12), which directs signatory nations to establish laws sufficient to ensure that legal persons (companies or organizations) may be held civilly, administratively, or criminally liable for cybercrimes if: (1) committed for their benefit by any natural person acting on their own or on behalf of the organization, or (2) lacking supervision or control by someone in a leading position (usually an officer or director) makes possible the Commission of a cybercrime that benefits the legal person.23

The CoE Cybercrime Convention is the first multinational treaty addressing cybercrime issues and is poised to become a global benchmark for cybercrime legislation in both industrialized and developing countries.

23The purpose of Article 12 is to ensure that legal persons (companies and corporations) may be held liable for the same offenses that may be committed by an individual when leading persons in such corporations commit these crimes on behalf of the corporation.
3. Other Council of Europe States

Although many CoE Convention signatories already have some form of computer crime laws in place, most will need to dramatically revise or expand their existing laws in order to meet the requirements of this treaty. France and Germany both have limited cybercrime laws that make it a criminal offense to gain unlawful access to data and to modify and distort such data. In addition, several CoE Member States have some existing laws that mention computer crime, but in most cases this is nothing more than a single provision of the penal code that makes it an offense to gain unauthorized access to a computer system.24 The remaining members do not appear to have any laws in place at this time. The important long-term message to developing countries (whether CoE members or not) whose cybercrime laws do not comport with the Convention is that they risk being considered a less secure place in which to conduct business because the data and systems within their borders will not be as protected. This means less foreign direct investment and domestic ICT opportunities.

D. ASIA-PACIFIC—LAWS ON CRIMES AGAINST COMPUTER SYSTEMS

1. Australia

In the Asia-Pacific region, Australia has enacted the comprehensive Cybercrime Act of 2001 (Cybercrime Act).25 While it does not contain the concept of a “protected” computer, there are similarities in approach to the U.S. Computer Fraud and Abuse Act. As seen below, most sections of the act apply to computers that either belong to the government or that are accessed by means of a telecommunications service. The scope of the act is broad. Offenses under it include:

- Knowingly causing unauthorized access to, or modification of, data held in a computer or unauthorized impairment of communications to or from a computer, when the unauthorized access, modification, or impairment is caused by means of a telecommunications service and with the intent to commit a serious offense.

---

24These countries are: Austria, Belgium, Czech Republic, Denmark, Estonia, Finland, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Switzerland, Spain, Turkey, and the Ukraine.

■ Knowingly or recklessly causing the unauthorized modification of computer data when such data is held in a government computer or is held on behalf of the government and the modification is caused by means of a telecommunications service or by means of a government computer.

■ Knowingly impairing data by means of a telecommunications service or by a communication sent from a government computer.

■ Knowingly accessing or modifying unauthorized restricted data held in a government computer or held on behalf of the government, or when done by means of a telecommunications service.

In addition, the Cybercrime Act covers (a) the unauthorized impairment of data held on a computer disk owned by the government, (b) possession of data with intent to commit a computer offense, and (c) supplying data with the intent to commit a computer offense.

Those convicted of an offense under the Cybercrime Act are subject to prison terms between two and ten years for each offense.

2. Japan

Japan has adopted a technical, specific approach to defining computer crime in the Unauthorized Computer Access Law of 1999, covering the same basic areas as the United States’. There are sections covering unauthorized access to a computer, trafficking in “personal identifiers” (such as ID/passwords), intentional interference with the performance of a computer system, computer fraud, and obtaining unlawful profit by introducing false information in a computer used for business. Those convicted of an offense under the law may be subject to imprisonment for up to one year and fines up to 500,000 yen.

3. Singapore

Singapore has adopted the Computer Misuse Act of 1993, which has been amended several times over the intervening years. In many ways it serves as a good model for a thorough cybercrime law. This law makes it an offense to (a) obtain unauthorized access to computer material (for example, software, data, computer resources); (b) to

---


27 Singapore’s Computer Misuse Act of 1993 can be found at http://agcvldb4.agc.gov.sg/non_version/cgi-bin/cgi_retrieve.pl?actno=REVED50A&doctitle=COMPUTER%20MISUSE%20ACT%0a&date=latest&method=part.
access computers with the intent to commit or facilitate another offense; (c) to modify without authorization computer material; (d) to use or intercept computer service without authorization; (e) to obstruct others’ permitted use of a computer without authorization; and (f) to disclose access codes without authorization.

Those convicted of an offense under the Computer Misuse Act may be subject to fines ranging up to S$50,000 and prison terms of up to ten years. Those convicted of an offense involving a “protected computer” under this law (that is, a computer involved in national defense, international relations, law enforcement, public safety, communications infrastructure, banking and financial services, public utilities, public transportation, or public key infrastructure) may be subject to fines totaling S$100,000 and prison terms up to 20 years. The act has extraterritorial application, allowing Singapore authorities to proceed against acts or actors originating outside the country but having an effect within Singapore’s borders.

III. Laws on Crimes against Communications Systems

A. INTRODUCTION

All electronic communications, whether voice, text, wire, or wireless, can be thought of as having two components: content and traffic data. The first item is the message itself, while traffic data are the dialing, routing, addressing, or signaling information that allows the message to get to its destination. In addition to being transmitted in real-time, each of these components may be stored somewhere along the transmission path. For example, e-mail texts are often stored in network systems, while recordings of voice telephone calls (as opposed to voice mail) are not. Conversely, records of traffic data or “toll records” for local and long-distance telephone calls are often maintained by communications providers for billing purposes, while Internet interconnection data is not generally retained for long periods of time. Finally, as in any business context, service providers maintain certain records about their customers (name, address, telephone number, IP address, and so forth) that in the electronic communications context are referred to as “subscriber information.”

To protect the privacy and integrity of each of these forms of electronic communications data and to facilitate law enforcement efforts, many countries have enacted what have come to be known as wiretapping, pen register, and trap-and-trace laws. These laws criminalize (a) the interception of the content of electronic communications as it is transmitted (wiretapping); (b) the capture of
outgoing and incoming traffic data (pen register and trap-and-trace\textsuperscript{28}); and (c) the access to or disclosure of stored electronic communications wherein the person intercepting, capturing, or accessing the particular form of data has no authority to do so. Such authority can be granted by law (in the case of a regulator or police official), by contract (as a condition of providing a communication service), or by consent (depending on the applicable law, from one or both of the parties to the communication). As criminal violations, the acts of interception, data capture, and access or disclosure must be intentional, willful, or otherwise convey the notion of conscious wrongfulness on the part of the actor. Also, in order to be illegal, these acts must be conducted without any form of authorization, whether legal, contractual, or consensual.

Frequently, the establishment of these criminal offenses is contained in the same statute that prescribes procedures for court-approved and other legal and permissible interceptions, captures, or disclosures of communications and data. In effect, the absence of such legal authorization or condition becomes an element of the criminal offense, rather than requiring the legal authorization to be asserted as a defense to the criminal charge. Accordingly, legal regimes that use this model make it illegal to intercept, capture, access, or disclose such information content, traffic data, or stored communications except in certain enumerated and sometimes elaborately articulated circumstances. These circumstances vary from country to country but will generally include access by regulators and/or law enforcement, monitoring by service providers to ensure and protect the quality of service, and access with the consent of one or more parties to the communication.

In addition to criminal sanctions, civil liability often attaches for illegal interceptions, captures, and disclosures of information whether by individuals, service providers, or government officials. This discussion will limit itself to criminal liability. Further, there is a distinction between illegally obtaining access to information and illegally disclosing such information. Communications or other information might be intercepted or obtained legally, but subsequently disclosed illegally. Against this backdrop, there are several illuminating examples of how legal systems around the world appropriately address these particular crimes.

\textsuperscript{28}Pen registers are devices that record the numbers dialed on a telephone (outgoing calls), and trap-and-trace devices identify the originating number (incoming calls). Pen register and trap-and-trace laws enable law enforcement to trace communications, not the content of communications.
B. NORTH AMERICA—LAWS ON CRIMES AGAINST COMMUNICATION SYSTEMS

1. United States

(i) Wiretaps

In the United States, there are three principal sections of the federal criminal code that prohibit interceptions, disclosures, and captures of electronic communications, whether wire-line and wireless telephony, voice mail, e-mail, or data transmissions. The Electronic Communications Privacy Act (ECPA) enacted the key provisions of the code governing wiretapping, pen registers, trap-and-trace devices, and access to or disclosure of stored communications information.

The basic U.S. wiretap law provides that, except as allowed in other subsections, it is a crime to:

- Intentionally intercept wire, oral, or electronic communication by an electronic, mechanical, or other device.
- Intentionally disclose communication contents known to be the result of an illegal interception.
- Intentionally and knowingly use information obtained by illegal interception.
- Intentionally and knowingly disclose communications obtained pursuant to a legal wiretap in a criminal investigation with the intent to impede such investigation.

The maximum penalty for violation of the wiretapping law is a fine of up to US$250,000 and not more than five years’ imprisonment. The exceptions to the general rule describe when these acts “shall not be unlawful.” These include:

- Actions by service providers necessarily incident to the provision of service or the protection of their property.

---

29 For other useful information, see http://www.cybercrime.gov/.  
30 18 U.S.C. Section 2511; the text of this provision can be found at http://www4.law.cornell.edu/uscode/18/2511.html.  
31 18 U.S.C. Section 3123; the text of this provision can be found at http://www4.law.cornell.edu/uscode/18/3123.html.  
32 18 U.S.C. Sections 2701–2702; the text of these provisions can be found at http://www4.law.cornell.edu/uscode/18/2701.html and http://www4.law.cornell.edu/uscode/18/2702.html, respectively.  
33 18 U.S.C. Section 2511(1); the text of this provision can be found at http://www4.law.cornell.edu/uscode/18/2511.html.  
34 18 U.S.C. Section 2511(2)(a)–(2)(i); the text of this provision can be found at http://www4.law.cornell.edu/uscode/18/2511.html.
• Actions pursuant to court order (note that wiretaps are only allowed in the investigation of certain federal crimes, which are listed in Section 2516(1) of the law and certain state crimes as described in Section 2516(2)).
• Emergency actions pursuant to a certification of the Attorney General of the United States in certain limited cases.
• Actions under the provisions of the Foreign Intelligence Surveillance Act.
• Actions by officials of the Federal Communications Commission.
• When one is a party to the communication, although some U.S. state laws require the consent of both parties to a communication before it can be recorded.
• When one has the consent of one of the parties (note, in several states, that consent of both parties is required).
• When the actions involve certain publicly available radio transmissions (pager messages and cordless calls, for example, are protected and cannot be lawfully intercepted).
• When a pen register or trap-and-trace device is being legally used.
• When law enforcement intercepts a computer trespasser.35

(ii) Access to and Disclosure of Stored Communications Data
The provisions of ECPA governing conduct other than interception of content follow similar rules. Section 2701, for example, prohibits intentional access to stored electronic communications without authorization, while Section 2702(a) provides that a public service provider may not knowingly divulge: (1) the contents of communication in electronic storage, (2) the contents of communications carried or maintained on that service, or (3) customer or subscriber information. Section 2702(b) lists exceptions for voluntary disclosure of such information. Section 2703 sets forth circumstances in which communications and records must be disclosed to governmental entities. Disclosure is either permitted or required (1) when there is customer or subscriber consent; (2) when related to the provision of service or the protection of the communication provider's rights and property; (3) when provided to law enforcement or other governmental entities pursuant to subpoenas, search warrants, court orders, or other statutory authorization; or (4) when reasonably necessary in an emergency involving death or serious injury.36

35 This provision was added through amendments made to ECPA by the USA PATRIOT Act.
36 This provision was added through amendments made to ECPA by the USA PATRIOT Act.
Section 2701 violations are punishable by criminal fines and/or imprisonment up to one year, or up to two years if a second offense. Section 2707 allows a civil action to be brought by the aggrieved party for actual damages suffered and any profits made by the violator, but in no case can a person entitled to recover receive less than US$1,000. Punitive damages are also available under this statute. Section 2702 violations are only subject to civil action.

**(iii) Pen Register and Trap-and-Trace**

Section 3121(a) of the federal criminal code provides that no person may install or use a pen register or trap-and-trace device without a court order. Three exceptions are provided for: (1) when the trap-and-trace device is used to operate, maintain, and protect service provider rights and property; (2) when it is used to record usage to detect and prevent fraud against service providers; or (3) when it is used with the consent of the user of the service. Otherwise, “knowing violations” of 3121(a) are punishable by a fine of up to US$100,000 and imprisonment of up to a year.

2. Canada

Sections 183 to 196 of the *Criminal Code of Canada* deal with the unlawful interception of private communications, with the principal pertinent provisions set forth in Section 184.37 Section 184(1) provides for the prosecution and punishment of the willful interception of private communications by means of any electromagnetic, acoustic, mechanical, or other device, with up to five years’ imprisonment. Subsection 184(2) provides exceptions to this rule if (a) the person intercepting the communication has the consent of the originator or if the originator intended the interceptor to receive the communication, (b) the interception is pursuant to legal authorization, or (c) the interception is necessary for service providers to provide or monitor service or to protect their rights and property. Section 184.1 sets out the circumstances for “an agent of the state” to intercept. Section 184.2 allows interception where authorization has been obtained from a judge, and Section 184.4 provides for emergency interceptions by peace officers in situations of potential serious bodily harm.

---

37*Criminal Code of Canada*, Sections 183–196. These sections fall within Part VI of the *Criminal Code of Canada*, which is entitled Invasion of Privacy. The text of these statutes and descriptions of related policy work currently under way at the Canadian Justice Department can be found at http://lois.justice.gc.ca/en/C-46/38885.html.
Section 492.2 of the Criminal Code provides for the issuance of a judicial warrant to install a “number recorder,” similar to a pen register and trap-and-trace device.38

C. EUROPE—LAWS ON CRIMES AGAINST COMMUNICATION SYSTEMS

1. European Union

While not a criminal statute, the EU has had in force for several years a Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector39 (the Directive), which precludes transmission of personal data outside the EU unless the receiving country provides adequate protection of the data consistent with the terms of the Directive. EU Member States are required to harmonize their domestic laws with the Directive. The EU recently extended the Directive to cover all electronic communications.40 The Directive requires that the confidentiality of communications be ensured and that traffic data be deleted or made anonymous at the conclusion of a communication, except as necessary for billing and other limited purposes. To avoid undue difficulty for law enforcement, the Directive contains provisions that allow countries to derogate from these requirements in order to permit interceptions of communications and

retention of traffic data for the investigation of crimes and the protection of national security.

Other EU initiatives are under way: The European Commission has issued a *Communication on Cybercrime*, which discusses the need to balance privacy and law enforcement interests. The EU has also proposed a *Framework Decision* to approximate the criminal laws of the Member States on attacks against information systems.\(^\text{41}\)

2. Council of Europe

Article 3 of the Council of Europe *Convention on Cybercrime* requires all signatory nations to criminalize interceptions that are “intentional” and “without right.” Paragraphs 38 and 51 to 59 of the Explanatory Memorandum indicate that the words “without right” are intended to allow Member States and signatories great flexibility in detailing the circumstances in which interceptions may be permitted, including the exclusions and exceptions discussed above.\(^\text{42}\)

3. The United Kingdom

The U.K. *Regulation of Investigatory Powers Act* (RIPA) follows a pattern similar to that of the model discussed in Section A of Part III of this Chapter.\(^\text{43}\) Section 1, I, Part I of RIPA addresses communications content, and establishes the offense of “intentionally and without lawful authority” intercepting, “at any place in the U.K.,” any communication in the course of its transmission by “a public postal or telecommunication service.” RIPA also makes it an offense to intercept “any communication in the course of its transmission by a private telecommunications system” unless the interceptor is a person with a right to control the system, or has the consent of such a person. Exceptions are provided to this provision. Sections 3, 4, and 5 list additional circumstances in which interceptions are lawful. In general, the exclusions permit interception (1) where there is consent of the

---

\(^\text{41}\)These and other relevant materials on EU actions can be found at the provisional website for the EU Forum on Cybercrime, http://cybercrime-forum.cec.eu.int/default/.


communicating parties, (2) where necessary for monitoring of a system for security reasons and for protection of system rights and property, and (3) where the interceptor acts under judicial or executive orders.

Chapter II of RIPA addresses “Communications Data” (defined as traffic data and subscriber information). RIPA’s approach differs from models that make content interception illegal unless specifically authorized. Section 21(2) provides that the disclosure of communications data “shall be lawful for all purposes if . . . authorized by provisions of the Chapter.” The authorizations are governed by Sections 22 to 24 of RIPA, and generally allow disclosure if made in response to police and other executive officers, rather than judicial officers.

4. Germany

Under the 1996 amendments to the Telecommunications Act (the Telekommunikationsgesetz or TKG), and the Telecommunications Installation Act (the Fernmeldeanlagengesetz or FAG), any intentional and illegal interception of a communication message to a third party is a criminal offense. In the investigation of certain serious crimes, Sections 100(a) and (b) of the Code of Criminal Procedure provide for the interception of communications on public networks under judicial order. Information that some might consider to be “traffic data” or “stored communications” is, under the German law, subject to the same standard for access as communications content.

5. Italy

Under Italian law, interception of communications is only permitted by Article 266 of the Criminal Procedure Code in investigations of offenses with a maximum sentence of up to six years’ imprisonment.

D. ASIA-PACIFIC—LAWS ON CRIMES AGAINST COMMUNICATION SYSTEMS

1. Japan

Article 21 of the 1946 Japanese Constitution explicitly protects the secrecy of all communications without exception. Moreover, Article 104 of the Telecommunications Business Law and Article 14 of the Wire

---

44Germany’s TKG can be found at http://www.netlaw.de/gesetze/TKG.htm.; FAG at http://www.netlaw.de/gesetze/FAG.htm.
45Japan’s Telecommunications Business Law, Article 104 can be found at http://www.soumu.go.jp/joho_tsusin/eng/Resources/laws/TBL/Chap5.html.
Telecommunications Law prohibit interceptions by anyone. Therefore, wiretapping by law enforcement was extremely rare until 1999 when the Diet passed Japan’s first wiretap statute authorizing interception in organized crime cases involving designated offenses. Articles 3 to 6 of The Japanese Law on Communication Interception During Criminal Investigations describe procedures for obtaining a court-issued interception warrant. Article 16 allows for traces of incoming calls. Article 30 provides that a public officer who commits a violation of the Telecommunications Business and Wire Telecommunications laws shall be imprisoned for three years.

IV. Crimes Facilitated by Computers and the Internet

A. INTRODUCTION

In addition to those offenses specifically related to computer fraud and abuse and those that seek to protect the confidentiality, integrity, and availability of computer data or systems, there are also many traditional or “offline” offenses that can be facilitated by the use of computers or the Internet. Although these offenses are not the primary focus of this report, legislators and policymakers should take care to ensure that the laws and penalties governing such offenses are technology neutral and apply equally to both online and offline conduct.

In March 2000, the U.S. Department of Justice (DOJ) published The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet (the DOJ report). The report addresses many of the legal and policy issues surrounding the use of computers and the Internet to commit traditional offenses. The DOJ report concluded that substantive laws that regulate traditional offenses should ensure that online conduct is treated in a manner consistent with the way offline conduct is treated, that such laws are written in a technology neutral way, and that they take account of other important societal interests.

47The Diet is the Japanese national legislative body.
such as privacy and the protection of civil liberties. The DOJ report noted, at page 11:

If an activity is prohibited in the physical world but not on the Internet, then the Internet becomes a safe haven for that unlawful activity. Similarly, conduct that is not prohibited in the physical world should not be subject to prohibition merely because it is carried out in cyberspace.

Every jurisdiction should consider enacting laws that remove such unintended loopholes.

B. TYPES OF OFFENSES

In particular, the DOJ report analyzed existing U.S. federal laws in the following areas.

1. Fraud and Money Laundering

Fraud is increasingly committed through the use of computers connected to the Internet, and laws against such fraud should apply regardless of whether the conduct takes place online or offline. Internet fraud is defined as “any fraudulent scheme in which one or more components of the Internet, such as websites, chat rooms, and e-mail, play a significant role in offering nonexistent goods or services to consumers, communicating false or fraudulent representations about the schemes to consumers, or transmitting victims’ funds, access devices, or other items of value to the control of the scheme’s perpetrators.”

A prevalent and serious form of fraud is identify theft, in which personal financial data is obtained and then either nonexistent transactions are billed to the consumer or actual transactions are made using the consumer’s data. Identify theft, in particular, is a significant and growing problem that may require heightened investigative and prosecutorial attention. In October 2000, an international initiative involving five U.S. agencies, 23 states, and consumer protection agencies from nine countries unveiled 251 law enforcement actions targeting the top 10 online scams. The top 10 categories for online fraud are:

- Internet auction fraud

---


• Internet Service Provider scams
• Internet website design/promotions: web cramming
• Internet information and adult services: credit card cramming
• Multilevel marketing/pyramid scams
• Business opportunities and work-at-home scams
• Investment schemes and get-rich-quick scams
• Travel/vacation fraud
• Telephone/pay-per-call solicitation frauds (including modem dialers and videotext)
• Health care frauds.52

In the United States, cyber fraud is prosecuted primarily under consumer protection statutes enforced by the Federal Trade Commission and state attorneys general.

ICTs also play a role in each of the three stages of money laundering: (1) placement of the illegal funds into the financial system, (2) layering the funds through wire transfers and other mechanisms that complicate the trail, and (3) moving the laundered funds back into an economy. The Internet and new forms of digital money have added new facets to money laundering enforcement that present new, difficult challenges for all countries, but especially for developing nations.

2. Economic Espionage and Theft of Intellectual Property

Economic espionage, like fraud, is increasingly committed through the use of computers and the Internet. The United States enacted the Economic Espionage Act of 199653 to provide criminal penalties for theft of trade secrets, confidential and proprietary information, and for attempted theft and conspiracy to engage in theft, regardless of whether the theft, attempt, or conspiracy were accomplished by traditional means or via computers and the Internet and regardless of whether a domestic or foreign competitor, or a foreign government,

54The Economic Espionage Act of 1996 broadly defines “trade secret” to include “all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing.” 18 U.S.C. Section 1839, http://www.cybercrime.gov/eea.html.
was the perpetrator of the crime.\textsuperscript{55} The theft of intellectual property, including software piracy, can be a crime in many jurisdictions and is often facilitated by the use of computers and the Internet. Laws prohibiting the transmission of other content by computer, such as anticircumvention software, might also fall within this category.

As with laws seeking to detect and deter Internet fraud, it is important that laws protecting intellectual property, trade secrets, and confidential and proprietary information apply online and offline in both domestic and foreign jurisdictions, lest they end up deterring business investment and expansion.

3. Child Pornography and Obscenity

Child pornography and obscenity is also a large and growing problem, particularly given the ease with which such images can be created, stored, and distributed by computers or the Internet. Existing laws should be carefully scrutinized to ensure they cover such conduct.

4. Child-Sex Tourism, Prostitution, and Enticing of Minors to Engage in Sexual Activity

Nations without strong prohibitions and enforcement of child sexual abuse and child prostitution have become attractive tourist destinations for people who engage in this type of conduct. Sites from these countries boldly advertise and enable itineraries to be arranged via the Internet. Increasingly, minors in industrialized and developing nations are lured into illicit sexual activity through chat rooms, e-mail, and other web-based interactions. Developing countries should take special precautions in their laws and regulations to prohibit these types of activities or they risk their ability to attract legitimate businesses that offer economic and social benefits to the country.

5. Sale of Regulated Items

The sale of prescription drugs, controlled substances, and other regulated items (such as alcohol and firearms) can occur without effective regulation if facilitated by computers or the Internet. Even if general laws that regulate such conduct are technology neutral, the use of computers or the Internet to facilitate such conduct is likely to raise particularly difficult investigatory challenges, as discussed below and elsewhere in this report.

6. Online Securities Fraud

Online securities fraud can come in many different forms. The Internet has opened up many new avenues for securities fraud including market manipulation, offering fraud (this can include fraudulent offerings of nontraditional stock as well as Ponzi schemes), and illegal touting (making statements that inflate perceived value of a stock without the legally required disclosure regarding the nature, source, and amount of compensation given in exchange for the positive comments). Chat rooms, spam e-mails, and e-newsletters are increasingly being used as vehicles to perpetrate securities fraud. Internet-related stock fraud is the second most common form of investment fraud, costing investors an estimated US$10 billion per year (or US$1 million per hour).\(^\text{56}\) In one U.S. case, a 23-year-old college student pled guilty to issuing a false news release over the Internet about Emulex Corporation, stating the company’s CEO had resigned. The news caused the company’s stock to drop by 50 percent in 15 minutes and cost investors more than US$110 million.\(^\text{57}\)

The existing securities laws have so far been sufficient to allow for the successful prosecution of these types of crimes, but as experience with handling them increases, additional legislation may be needed.

7. Use of Access Devices for Fraud and Related Activity

Specific U.S. laws address two classes of traditional crimes facilitated by computers. The first is the use of access devices for fraud and related activity.\(^\text{58}\) This statute makes it an offense to produce, use, or traffic access devices and telecommunications devices with the intent to defraud. Fraud is frequently committed using counterfeit access devices or telecommunications devices that have been altered to obtain unauthorized use of telecommunications services. Therefore, laws that render this behavior criminal are important deterrents.

8. Other Offenses

This list of traditional offenses that can be committed or facilitated online could readily be supplemented by adding:

- Blackmail, extortion, and other threats communicated by e-mail or other forms of electronic communication.

---


\(^\text{58}\)18 U.S.C. Section 1029; the text of this provision can be found at http://www4.law.cornell.edu/uscode/18/1029.html.
- Export or other trade-control violations.
- Forgery, counterfeit documents, digital manipulation of images or documents, and alteration of evidence by electronic means (with the requisite level of intent).
- Prohibited business transactions.
- Terrorist offenses and other national security violations.
- Unfair and deceptive trade practices.

C. RESPONDING TO INVESTIGATORY CHALLENGES

The use of computers and the Internet to commit traditional crimes raises important and difficult investigatory challenges. These challenges can arise from the unique nature of evidence stored on computers or transmitted over networks and the ease with which such evidence can be created, stored, copied, and transmitted. Such challenges may require that greater resources and improved training be directed toward computer forensics and other investigatory capabilities. Laws governing the investigatory powers conferred on law enforcement authorities may need to be revised. Any revisions should be carefully considered to assess the actual need for such additional powers, the potential for their abuse, and their potential impact on other important societal values.

V. Authentication and Security Laws

Nations seeking to establish laws protecting computer systems, information assets, and critical infrastructure, and thereby foster development and investment, often supplement their cybercrime laws with additional laws and regulations establishing secure and authenticated electronic transactions and messaging. Included, are laws promoting digital signatures and electronic authentication,59 laws promoting encryption,60 and relaxed encryption export/import controls.61

---

The most common mistake developing countries make is to assume that digital or electronic signature laws require a complex government-controlled structure for public key infrastructure (PKI) encryption technologies. It is also common to see developing countries require certificate authorities to obtain licenses. Such legal frameworks will deter foreign investment and will discourage the use of ICTs generally. The UN, EU, and U.S. digital signature laws all specifically require technology neutrality, meaning any type of authentication technology should be able to be used within the framework of the law. Countries whose laws mandate PKI authentication schemes will have laws that are not in alignment with industrialized nations and the global developing ICT legal framework.

Likewise, countries that place controls on the use of encryption technologies or require key escrow or key disclosure will also be perceived as a disadvantageous jurisdiction in which to do business. Only a few governments strictly control the use of encryption technologies, although many countries have export controls on strong encryption technologies with dual-use capabilities for military and commercial purposes.

VI. Conclusion

Nations looking for guidance on effective laws for combating cybercrime will find useful models and approaches in the laws and regulations of the countries and multilateral organizations discussed herein. It is not too late for developing nations in particular, and all nations generally, to adopt and improve national legal regimes supporting the security and integrity of computer and communications systems, information assets, and critical information infrastructure. If anything, the time to act is now. Subsequent chapters of this book will move from this discussion of a legal infrastructure for combating cybercrime to practical discussions of implementing anticybercrime laws and enforcing them within and among nations.
I. Introduction

A. JURISDICTIONAL ISSUES GENERALLY

Even before computers became a part of everyday life, traditional criminal cases often involved issues of jurisdiction. Probably the most common—and complex—jurisdictional issue involves conflicting laws among two or more countries, where action may be illegal in one country but legal in another. Other jurisdictional issues may arise when the accused is located in one country but the victim resides in another. The accused and victim may be in the same jurisdiction, but evidence of the crime may be maintained abroad. Additionally, the offense itself could involve more than one jurisdiction, as in a telemarketing scam or fraud operation whose participants and victims are scattered around the world.

The combinations are endless, and when such jurisdictional issues occur, they depend on the cooperation and legal systems of the countries involved to resolve them. They require, first and foremost, cooperation in the investigation and prosecution of the offense. This

may require law enforcement to address practical questions, such as which jurisdiction should take the lead. Courts and prosecutors may have to consider whether they have jurisdiction over the accused and whether the act in question constitutes an offense under domestic laws.

Because such cases often depend upon being able to gather evidence located in another country or state, the international community has developed longstanding methods for obtaining and providing legal assistance. The most common are the Letters Rogatory process and Mutual Legal Assistance Treaties (MLATs), often negotiated on a country-to-country basis. Where the goal is to prosecute an accused located abroad, there also needs to be a way to secure that person's extradition: Countries negotiate extradition treaties that govern how to make and respond to extradition requests. Jurisdictional issues are not new; the Internet, however, complicates them and increasingly brings them to the forefront.

B. JURISDICTIONAL ISSUES IN CYBERCRIME CASES

With the proliferation of computers and the widespread use of the Internet, jurisdictional issues are increasingly taking center stage. Over the past decade, the Internet and other communications technologies have been promoting advances in every aspect of society and every corner of the globe: They have been fostering commerce, improving access to information, and facilitating global communications. Governments, businesses, and consumers around the world have come to depend on computer networks as an efficient way to communicate and do business, but while the global and borderless nature of the Internet presents new opportunities for commerce, it also presents significant challenges for law enforcement, prosecutors, and the judiciary.

Unfortunately, many of the attributes of modern communications technology—such as low cost, ease of use, and the potential for anonymity—also make computers and the Internet an attractive medium for committing or facilitating crime. From the perceived anonymity of a home or library computer, a criminal can cross international borders with the click of a mouse. Law enforcement and investigators, however, cannot. They must resort instead to international law enforcement cooperation and often to time-consuming MLATs and Letters Rogatory.

While the procedure called for in MLATs may have worked well for 20th-century crime, it is often a hindrance in cybercrime cases because evidence is fleeting and investigators require access to
communications information in near real-time. The G-8 recognized these potential problems as early as 1996, in its recommendations to fight transnational organized crime, and in 1997, when Justice and Interior Ministers of the G-8 met to address high-tech crime. Several of their agreed upon action items included the development of expedited procedures for making mutual legal assistance requests in cybercrime cases. Since then, a number of international initiatives have tried to address the jurisdictional challenges posed by cybercrime, the most extensive being the Council of Europe Convention on Cybercrime. In addition to creating a range of cyber offenses and providing for broader procedural powers to gather electronic evidence, signatories now have an additional vehicle through which to address many of the jurisdictional questions tied to cybercrime.

C. CHAPTER OVERVIEW

This chapter describes the jurisdictional issues that may hinder the investigation and prosecution of cybercrime that crosses international borders and the ways in which law enforcement, the private sector, and the international community are coming together to address these jurisdictional constraints. Part II introduces the traditional methods of obtaining extradition and international legal assistance and describes why these traditional methods may not be adequate in the context of cybercrime. While it describes the legal and practical challenges faced by law enforcement and the courts, it also remains focused on how cybercrime can involve multiple jurisdictions at any given time. Part III addresses jurisdictional and conflict-of-law considerations as well as other considerations in cybercrime matters. Part IV describes what action is being taken around the world to address cybercrime-related jurisdictional issues and provides examples of how law enforcement and the private sector are using their cross-border networks to tackle cybercrime.

II. International Legal Assistance

A. INTRODUCTION

The best way to illustrate the cross-border issues that so often beset investigators in cybercrime cases is to consider a hypothetical example such as online credit card fraud. One of the reasons this form of fraud has skyrocketed is the ease of reaching a global net of victims without ever having to know their names, go to the bank issuing the cards, or
even set foot in their country. From a law enforcement perspective, this means that both victims and suspects can be scattered around the globe. Several countries may have an interest in seeing the case brought to trial. Which country, however, should take the lead? Furthermore, what happens if some of the countries involved do not have laws that would capture online fraud? What if their laws do cover the scam, but their substantive or procedural laws conflict? And what happens when investigators in North America, for example, learn that the suspects routed their communications through several countries in Europe and maintained detailed records of the scheme on servers in the Caribbean?

The possibilities are endless, but they are not uncommon. Cybercrime investigators encounter such hurdles every day. The problem comes with procedures associated with MLATs and Letters Rogatory that do not always meet the requirements of cybercrime cases. They can be time-consuming and may not provide the best means of dealing with electronic evidence. The following sections describe these procedures and then outline their shortcomings in the cybercrime context.

B. TRADITIONAL METHODS OF SECURING INTERNATIONAL LEGAL ASSISTANCE

1. Mutual Legal Assistance Treaties (MLATs)

The most common mechanism for obtaining international legal assistance is the voluntary cooperation between governments. In joint investigations, for example, MLATs are not usually needed. If the conduct also violates the other country’s laws, it can simply open a domestic investigation and share information.

MLATs are used when there is no legal basis to otherwise cooperate on legal assistance matters such as the issuance of subpoenas, interviewing witnesses, the search or seizure of evidence, or the production of documents. MLATs are treaties that outline procedures for gathering evidence in a foreign nation and provide for direct communication between the central authorities of the countries party to the agreement. Under the MLAT process, law enforcement agencies may not necessarily communicate directly.

2The United States, for example, is party to 44 bilateral MLATs presently in force. Other MLATs have been signed but have not yet been ratified by the Senate. In addition, the Office of Internal Affairs in the Criminal Division of the Department of Justice is constantly working on developing new MLATs. The United States has more than doubled the number of MLATs in force since 1997.
MLATS are usually bilateral treaties negotiated between countries to create a mechanism for cooperation where one may not otherwise exist. They do not, however, ensure cooperation. For example, essential-interests sections of MLATs allow countries to opt out of cooperation. The primary advantage of MLATs is that they formalize the relationship. Other vehicles, such as Letters Rogatory (discussed below), rely instead on the principle of comity; thus the country that receives the request is not obligated to comply.3

MLATs are not without drawbacks, one of the most significant being the time factor. While requests may be processed relatively quickly, most are often executed too slowly. The courts in the foreign country, for example, often have to issue legal documents formally authorizing the request. This legal process is subject to potentially time-consuming challenges and appeals.

MLATs also carry their restrictions. For example, some MLATs require dual criminality and/or that the offense be extraditable.4 “Dual criminality” means the act under investigation must be criminalized under both countries’ laws and punishable by a minimum term in prison, usually one year. If the act being investigated does not meet that requirement, the country receiving the request does not have to fulfill it. Other MLATs permit assistance involving subpoenas, interviewing witnesses, or search and seizure or production requests if the crime is an offense in the requesting state. “List MLATs” set forth a list of offenses to which they are applicable.5

Each MLAT outlines the particular procedure for making a request for legal assistance. For example, requests from other countries to the United States are handled by the Office of International Affairs (OIA) in the Criminal Division of the U.S. Department of Justice. Likewise, when the United States needs assistance from a foreign country, the request usually follows a uniform process. Namely, the United States, as the requesting country, (a) sets out the facts of the case, (b) names the defendants or subjects, (c) provides information about witnesses or other entities in the foreign country, and (d) states the specific form of legal assistance requested. The OIA signs and sends the request and a

3Comity is the willingness to grant a privilege, not as a matter of right, but out of deference and goodwill.
4Extraditable offenses are those offenses for which a country will agree to extradite.
translation to the central authority of the foreign country, usually the Ministry of Justice. The foreign country then processes the request and collects and sends the evidence to the OIA, which in turn hands the evidence over to the prosecutor handling the case.

MLATs can also specify the desired criminal procedure to be followed in executing the request. For example, some require the requested country to gather the evidence in accordance with the requesting country’s procedures. Other provisions may require the requested country to produce evidence even if the disclosure of such information would violate its domestic privacy laws.

2. Letters Rogatory

If the countries in question do not have an MLAT between them, they can still seek and provide assistance through Letters Rogatory as provided by law. The Letters Rogatory process involves one country’s judicial authority making a request of another country for legal assistance in one specific case.\(^6\)

One of the drawbacks of seeking assistance through the Letters Rogatory process is that the country that receives the request is not obliged to comply. While it may agree to do what is asked, it does so only as a matter of comity, that is, as an international favor. Furthermore, Letters Rogatory are a diplomatic matter, which means they must be processed by the foreign and justice officials of both countries. Consequently, the process can be time-consuming and can hinder investigations. In this way, the Letters Rogatory process is less efficient than seeking a request through an MLAT.

3. Extradition

Extradition involves one country handing over an accused to stand trial for an offense in another jurisdiction. Extradition is customarily handled pursuant to a formal extradition treaty and is usually reserved for certain classes of offenses that are either listed in the treaty or meet a dual criminality criteria for crimes punishable by one year or more in prison. The offenses for which a country will extradite—extraditable

\(^6\)In the United States, for example, the Letters Rogatory process is authorized under U.S. law in 28 U.S.C. Sections 1781–1782. The text of these provisions can be found at http://www4.law.cornell.edu/uscode/28/1781.html and http://www4.law.cornell.edu/uscode/28/1782.html, respectively.
offenses—are usually set out in the extradition treaty through one of two approaches: enumerative treaties and eliminative treaties.

The first approach is to explicitly name the extraditable offenses, giving the countries the right to refuse extradition if the offense in question is not recorded in the treaty. This type, referred to as an “enumerative” or “list” treaty, is typical of older agreements. It has fallen out of favor, however, because of the risk of rendering the treaty ineffective through inadvertent omissions or changes in substantive criminal laws.

Today the preferred approach is to enter into “eliminative” treaties. Eliminative treaties provide for extradition for any offense in which there is dual criminality. Dual criminality may not be an issue when the two countries have similar legal systems and laws, but it creates problems when the countries have inconsistent or conflicting substantive laws. Cybercrime presents especially difficult problems here because laws regarding the use of ICTs are still evolving and there is little global consensus on standards and levels of punishment. As a result, the better way to handle outdated enumerative treaties is not to transform them into eliminative treaties, but rather to add “computer-related offenses” (or equivalents) to their lists of extraditable offenses to avoid dual criminality issues.7

To complicate matters further, countries commonly will not allow extradition of their own citizens.8 They also may refuse if the alleged offense is not a crime under their laws or is considered to be a minor offense.

C. PROBLEMS WITH TRADITIONAL METHODS IN CYBERCRIME CASES

1. The Country Whose Assistance Is Required May Not Have Adequate Procedural Laws

International computer crime investigations can be hampered by inadequate procedural laws. Even if the countries involved have formal legal assistance treaties in place or obtain a Letters Rogatory, this may not be enough if the country whose assistance is sought is not also empowered to do what the requesting country asks. For example,

---

8The United States, however, does allow extradition of its citizens.
if the country asked to gather evidence has no procedural mechanism for obtaining evidence stored within its borders or for compelling service providers who hold the information to cooperate, the investigation may be thwarted notwithstanding the presence of mutual legal assistance agreements or Letters Rogatory from the court of that country. The CoE Cybercrime Convention attempts to address this issue by outlining minimum standards for procedural powers in cybercrime cases.

Procedural problems are not limited to cases involving international legal assistance. Computer communications cross international borders, as well as state or provincial borders, with ease. In the United States, for example, state investigators often serve subpoenas for information on Internet Service Providers that are not located in their state. However, the United States has no formal procedural mechanism for service and enforcement of one state’s subpoena in another state. Similarly, there is no legal mechanism for enforcing an electronic surveillance order in another state, and state investigators must either obtain a federal order or an order under the law of the state in which the provider is located. Recent changes to U.S. federal law have helped, at least with federal criminal investigations. Under amendments contained in the USA PATRIOT Act, pen register and trap-and-trace orders now have nationwide service; formerly, the government was forced to get an order from the court who had jurisdiction over the service provider (where the service provider records were located), regardless of the location of the investigation. Search warrants for electronic evidence and orders for transactional information now also have nationwide service, obviating the need for the government to obtain an order in each district in which evidence is found—thus making it easier for the federal government to investigate cyber criminal activities.

2. Law Enforcement May Not Have Sufficient Technical Expertise

While not necessarily a strict jurisdictional issue, the technical expertise of law enforcement, prosecutors, and judicial officers clearly affects the ability to obtain international legal assistance. Law enforcement officials requiring international legal assistance must rely not only on the willingness of those countries to cooperate, they must also contend with the technical and legal ability—or inability—of foreign law enforcement to provide that assistance. Even if a foreign country is

---

9CoE Convention, Articles 14–21.
willing to cooperate in a cybercrime investigation, many law enforcement agencies around the world lack the technical knowledge, equipment, and funding to be of much assistance. Cyber investigative and forensic education is costly and continuous. Furthermore, the difficulty of retaining technically qualified agents could prove prohibitive for countries trying to fight cybercrime.\textsuperscript{10} Even countries such as the United States have a shortfall of skilled cyber investigative experts and have trouble funding continuing education for the personnel they have.\textsuperscript{11} Some developing countries similarly may be unable to keep pace.

Law enforcement agencies are not the only ones that need to be technically savvy. In order to assist foreign agencies in resolving jurisdictional issues, prosecutors and judges must understand how ICTs impact the legal and judicial system. Training may be sparse or nonexistent. As a result, cybercrime investigations relying on foreign assistance can be stymied by a lack of resources at critical levels despite the willingness to help.

3. Traditional Mechanisms May Be Too Slow and Cumbersome

Even with complete cooperation between countries, electronic evidence can disappear in an instant. Because cybercrime cases are so fast-moving and electronic data is so transitory, most cybercrime investigations will require an expedited means of obtaining assistance from other jurisdictions. The CoE Cybercrime Convention recognized the need for expedited forms of assistance; this was also the driver behind the G-8 24/7 Point-of-Contact Network. Developing countries would do well to establish mechanisms for prompt assistance to international cybercrime investigative requests.

III. Jurisdictional Considerations and Conflicts of Laws

A. INTRODUCTION

Traditional methods of securing assistance or extradition may not be adequate in the cybercrime context. Obtaining legal assistance from other jurisdictions is only the first step in bringing cross-border cybercrime cases to trial. Even where foreign countries agree to provide


assistance and their law enforcement agencies have sufficient resources
and training to do so, jurisdictional and conflict of laws issues can
create significant problems in the investigation and prosecution of
cross-border cybercrime. This section outlines some of the challenges
that make cybercrime cases particularly difficult.

B. DISCUSSION

1. Traditional Mechanisms May Not Be in Place

Many countries may not have MLATs or extradition treaties with the
country whose assistance they require. The United States, for example,
presently has just over 40 MLATs in place. Thus, critical evidence may
not be obtainable in countries where there is no formal assistance
mechanism. Sophisticated cyber criminals are well aware of these
limitations. The CoE Cybercrime Convention attempts to address this
issue. Chapter III of the treaty sets forth general principles relating to
international cooperation, extradition, and mutual assistance.12 It
states, for example, that “[t]he Parties shall afford one another mutual
assistance to the widest extent possible for the purpose of investigations
or proceedings concerning criminal offenses related to computer
systems and data, or for the collection of evidence in electronic form of
a criminal offense.”13 Signatories to the CoE Convention that do not
have an extradition treaty between them may treat the Convention as
the legal authority for extradition.14

2. The Act Might Not Be Considered an Offense

Cybercrime cases are often complicated by inconsistent legal
frameworks, particularly when the suspect lives in a country that does
not have adequate laws. While most industrialized countries have been
struggling to update their criminal laws to cover computer-related
crimes, some developing countries do not criminalize computer-related
offenses, such as hacking, spreading of viruses, or theft of data. The
gaps in their criminal laws affect not only their ability to fight
cybercrime within their own borders; they also frustrate foreign
investigations and international initiatives aimed at tackling cybercrime
on a global level.

12CoE Convention, Articles 23–35.
13CoE Convention, Article 25.
14CoE Convention, Article 24.
MLATs and extradition treaties often require “dual criminality,” that is, the conduct being investigated must be a crime under the laws of the country requesting assistance and the country whose assistance is required. The lack of cybercrime laws in jurisdictions in which assistance is being sought is one of the most significant challenges in pursuing computer criminals. The problem has already stymied investigations in several highly publicized cybercrime cases.

**Case Examples**

- In 1992, hackers from Switzerland attacked the San Diego Supercomputer Center in California. The United States sought assistance from Swiss law enforcement; however, the MLAT between the United States and Switzerland required dual criminality. Because Switzerland’s laws did not criminalize hacking, official cooperation under the treaty was impossible. The Zurich police eventually provided assistance, but only after taking elaborate steps to ensure the proper investigation of the case. By that time, the hackers had ceased their operations and all the leads were cold. The U.S. government closed its case.15

- In an extradition context, an Argentinian named Julio Cesar Ardita was suspected of hacking into several military, university, and private computer systems in the United States. The United States wanted to extradite Ardita to be tried under U.S. law. However, the extradition treaty between the two countries contained a requirement for dual criminality. At the time, hacking was not a crime under Argentina’s law. As a result, it would not allow Ardita’s extradition.16

---

In perhaps the most high-profile case, the investigation into the I LOVE YOU virus was hampered by a lack of adequate computer crime laws in the Philippines. At the time, the law in the Philippines did not criminalize the conduct involved in creating and distributing a computer virus. According to former U.S. Deputy Assistant Attorney General Kevin DiGregory, “International coordination would have proceeded more quickly and effectively had there existed common computer crime laws between our countries.” Ultimately, the author of the virus was not prosecuted. The incident provided the impetus for increased cooperation at the global level as countries around the world were forced to acknowledge that the fight against cybercrime demands collaborative efforts. The Philippines has since enacted cybercrime laws that criminalize spreading viruses.17

The challenge for all countries will be keeping their laws up to date so they do not end up creating havens for bad actors. All countries need to work together to address cybercrime and to assist developing countries draft adequate cybercrime laws.

3. Enforcement in the Face of Conflicting Laws

Perhaps the greatest legal challenges in combating cybercrime are when both countries have conflicting laws concerning the matter at hand. Conflicts can arise in various ways, but usually involve viewing an activity as legal in the country where it takes place but illegal under another country’s criminal laws.

Hate speech and laws relating to the sale of Nazi memorabilia and related communications offer several recent examples. In some countries, such communications and conduct are illegal. In others, such as the United States, they are legal and, in fact, are protected under the constitutional right of free speech. The conflict with cybercrime issues is inevitable because Internet communications can originate in one country but be accessed in another, making the same conduct that is

protected under one country’s laws prohibited by another’s. In a high-profile example, German authorities sought assistance with investigations into hate speech because of what they saw as a rise of Nazi-related websites being hosted on U.S. servers. As speech alone, hate speech is not a crime in the United States and is considered to be constitutionally protected speech under the First Amendment to the U.S. Constitution. As a result, German authorities must devise other means to enforce German laws against hate speech in the United States or other countries who take a similar position.\(^{18}\)

These following example cases highlight the conflicts that can arise in pursuing cases across international borders. They go beyond activities prohibited in one country but legal in another. An even more difficult problem is the reverse: when complying with the laws of one country would be illegal under the laws of another.

**Conflict-of-Laws Case Examples**

- In perhaps the most high profile Internet-related case to date, Yahoo!, an Internet Service Provider based in California, sought a declaration from a California court on the validity of an order issued by a court in France. The French court ordered Yahoo! to block French citizens’ access to Nazi-related material displayed or offered for sale via its server located in the United States. The sale of Nazi-related items is protected in the U.S. by the First Amendment to the U.S. Constitution, but it is illegal under the laws of France. As a result, several French groups sued Yahoo! in France. While the French court’s order did not carry criminal sanctions, it imposed stiff monetary penalties for each day the ISP did not comply. Yahoo! responded by asking the California court for a declaration that the order was unenforceable in the United States. The district court found, indeed, that the French order was unenforceable against Yahoo! in the United States because it presented a real and immediate threat to its subscriber’s constitutionally protected right of free speech.\(^{19}\)

\(^{18}\)It is also interesting to note that freedom of expression is protected under international law. See also Friedrich Kubler, “How Much Freedom for Racist Speech?: Transnational Aspects of a Conflict of Human Rights,” 27 Hofstra Law Review 335 (1998).

Another case involved an Australian professor whose website contained comments denying the Holocaust. The professor’s comments were legal in Australia but were illegal under German law. As a result, a German court ruled that the comments amounted to an offense under German law because, having been posted to the Internet, they could be accessed in Germany.\textsuperscript{20}

In a case involving proceedings in the United States against the Bank of Nova Scotia (a Canadian bank), a U.S. court issued an order compelling the bank to produce bank records stored in the Bahamas. The Bank of Nova Scotia refused to comply, as doing so would violate a Bahamian bank-secrecy law. Despite the conflict with the Bahamian law, the U.S. court held the bank in civil contempt.\textsuperscript{21}

A similar problem often arises with conflicts of laws governing the protection and interception of data. By way of example, Internet chat, e-mail, and messenger services are available globally. For a U.S.-based ISP such as MSN and Yahoo!, while the services are available globally, the services and data storage are physically located in the United States. As a result, such providers are subject to U.S. law.

One such law is the \textit{Electronic Communications Privacy Act} (ECPA).\textsuperscript{22} ECPA prohibits disclosure of certain types of information to governmental entities without meeting a specified legal process. U.S. wiretap laws generally \textit{prohibit} the interception of communications absent an order from a U.S. court.\textsuperscript{23} Many other countries, however, such as the United Kingdom and Australia, have passed laws that \textit{allow} for the interception of communications. These laws provide for interception by service providers where the service is available in their country. As a result, a country such as Australia could serve a valid court order on a U.S.-based provider offering service in Australia, which, if complied with, would require action contrary to what is allowed under U.S. law. This illustrates how important it is for countries to work together to develop a consistent global legal framework.

As of yet, there is no easy way to resolve cases involving inconsistent or conflicting domestic laws. Principles of international comity generally apply, but the extent to which any state honors the judicial decrees of foreign nations is a matter of choice, governed by the comity of nations. Comity is neither a matter of absolute obligation nor of mere courtesy and goodwill. As the California court noted in the Yahoo! case: "Absent a body of law that establishes international standards with respect to speech on the Internet and an appropriate treaty or legislation addressing enforcement of such standards to speech originating within the United States, the principle of comity is outweighed by the Court’s obligation to uphold the First Amendment."24 Because Internet communications are inherently global, it is an issue that needs to be resolved at an international level.25

4. Establishing Jurisdiction in a Networked World

Jurisdiction over a person or thing traditionally depends on the physical presence of the person or thing within a country’s borders, even for a short or transitory time. While physical presence is a straightforward concept with respect to people and objects, it is harder to ascertain the location of data on electronic networks, creating jurisdictional confusion and disputes. For one thing, electronic data is arguably accessible from any point on the network. As networks make physical borders less relevant, other criteria for jurisdiction must be established. To this end, initiatives such as the CoE Convention on Cybercrime are providing the international community with valuable guidance.

In some cases, defendants have taken advantage of the still-evolving law in this area and have attempted to challenge a court’s jurisdiction by noting that they used a foreign server. While this argument is more common in civil cases, it is also increasing in the cybercrime context. In such cases, courts will need to consider whether this fact alone

25The negotiation over the Council of Europe Cybercrime Convention illustrates the difficulty of resolving issues such as these. While some members of the Council of Europe wanted to address issues such as hate speech in the Cybercrime Convention, other countries opposed the move. As a result, the issues will still be addressed, but not in the body of the Convention. They will be addressed instead in a protocol to the Convention. A preliminary draft dated June 21, 2002, is available from the Council of Europe’s website at http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Combating_economic_crime/Cybercrime/Racism_on_internet/AddProtCybercrimeE-4.pdf.
deprives them of jurisdiction over the accused. In a recent case in Norway, the court held that it did not; the defendant was convicted for online hate speech despite the fact that he used a foreign server.\footnote{26}{“Rare Case Has Norwegian Man Convicted of Racism on the Web,” Associated Press, Apr. 24, 2002, http://www.law.com/jsp/statearchive.jsp?type=Article&oldid=ZZZ2CYYEE0D; “Norwegian jailed for Web racism”, Apr. 23, 2002, cnn.com, http://www.cnn.com/2002/WORLD/europe/04/23/norway.web/ .}

In other cases, it is not the location of the data that complicates matters but rather the location of the accused and victim. In one case, for example, Canadian authorities initiated an investigation into a cyber stalking case of a Canadian victim. The woman, a well-known actress, became concerned after receiving increasingly threatening letters and e-mails from an Australian fan. Canadian investigators brought the case to the attention of their Australian counterparts, who charged the accused with violating Australia’s stalking laws. The case was dismissed, however, because the Australian court did not believe it had jurisdiction over the case. The court reasoned that, while the accused lived in Australia, the effects of his conduct were felt overseas. In other words, because the alleged harm was not felt in Australia, the court concluded it could not exercise jurisdiction over the case. The decision was overturned on appeal and the case was sent back to the lower court for trial. The accused, however, has appealed further; the outcome of the appeal is as of yet unknown.\footnote{27}{See Lesia Stangret, “Cyber-stalking ruling reversed: Australian to be tried in case involving Canadian actress,” National Post, Mar. 6, 2001, at C7; and Lesia Stangret, “Cyber-stalking Omen: Jurisdictional Woes Highlighted in Case Involving Canadian,” National Post, Feb. 9, 2001, at C7.}

If the appellate court is overturned, the accused will likely avoid trial. While Australia will be unable to prosecute on legal grounds, Canada is unlikely to pursue the case further for practical reasons. According to the lead investigator in Canada: “We would love to prosecute but we’re separated by 10,000 miles.”\footnote{28}{See Lesia Stangret, “Cyber-stalking ruling reversed: Australian to be tried in case involving Canadian actress,” National Post, Mar. 6, 2001, at C7.} Canadian authorities, he said, have taken out a country-wide warrant, but “[f]rom the Canadian side, we’ve done all we can do.”

In essence, the case could become one in which the accused’s home country does not prosecute because the victim lives abroad and the victim’s home country cannot pursue the case further because the accused lives overseas. There is no easy solution to this catch-22 that is a product of legal and practical cyber jurisdictional considerations. However, consultation between the countries at an early stage can help authorities identify potential problems and plan around them.
5. Cooperating with Other Countries That Have an Interest in the Case

Because digital information can be accessed almost anywhere in the world and may be routed through any number of countries, any investigation into a computer-related crime can end up involving multiple countries. Take the example of a child pornography ring operated in the United Kingdom, using communications services in the United States, and involving child victims from around the world. Arguably, the United Kingdom, the United States, and the victims’ home countries all have an interest in investigating and prosecuting the crime. Evidence of the offense may exist in each one. Which country, then, should pursue the case or have jurisdiction over the accused?

While there is nothing stopping any country from pursuing the case domestically (provided they have adequate laws to do so), foreign authorities would be wise to communicate and determine whether one or more should take the lead. In this context, the question is not only whether a country can exercise jurisdiction over the suspect or offense but whether other countries also have an interest in the offense and whether a cooperative approach can provide a better resolution. The CoE Convention encourages such consultations by requiring signatories to cooperate to the widest extent possible.29

6. Special Issue: Juveniles

Although it is impossible to survey or even anticipate all the issues that can arise in cross-border cybercrime cases, one last issue that deserves mention is the fact that computer-related offenses are often committed by juveniles. Jurisdiction over juveniles may vary from country to country, as can treatment of young offenders. As a result, where the offense is committed by a juvenile, the age of the suspect may pose an unexpected hurdle in investigating or prosecuting the case.

7. Encryption

Cryptographic systems can also stymie investigation of computer-related crime. The matter is complicated by different countries approaching encryption in different ways. A few, such as the United Kingdom, have adopted laws that require those with encryption keys to assist with the decryption of data or, in some cases, to actually hand the encryption

29CoE Convention, Articles 23, 25.
keys over to enable law enforcement to decrypt the evidence itself. Most countries, however, have adopted a hands-off approach, deciding the benefits of encryption to good actors outweighed the challenges to law enforcement. Ultimately, however, the time, effort, and expense of tracing digital communications—and securing, where necessary, international legal assistance—may be wasted if the data are encrypted and the agency lacks the technical or legal ability to decrypt them.

8. Different Standards in Relation to Privacy and the Retention of Data

Further issues arise over individual rights to privacy and protection of data. Data can be protected by constitutions, laws, regulations, case law (for common law jurisdictions), and contracts between parties. The 1997 EU Directive concerning the processing of personal data and the protection of privacy in the telecommunications sector\(^{31}\) is intended to protect personal data from misuse and requires the immediate deletion of all personal identifying information following the termination of a communication that is not needed for billing and other limited purposes. Amendments to the EU Directive have replaced the 1997 Directive and extended its scope to encompass the Internet (electronic communications).\(^{32}\) The U.S. Electronic Communications Privacy Act protects certain personal information from disclosure absent compliance with specified procedures. Therefore, requests for protected data are often challenged, sometimes by communications providers who fear liability if they disclose the information.

Lack of data retention creates the reverse problem: There are no data to obtain for evidence because they were not retained. Although

---

\(^{30}\)See, for example, the U.K.’s Regulation of Investigatory Powers Act 2000, 2000 Chapter 23 (in particular, Part III: Investigation of Electronic Data Protected by Encryption Etc.).


the CoE Cybercrime Convention does not mandate retention of data, it has a provision that can be triggered to enable government officials to require preservation of data.\textsuperscript{33} Government policies on the preservation or retention of data vary from one country to another. At present, the EU is leaning toward data retention, while the United States favors data preservation that requires a provider to preserve specific data on a case-by-case basis for a specified time to meet law enforcement or legal requirements.\textsuperscript{34} Opponents of data retention point out that business costs to meet retention requirements will be high and, ultimately, will be passed on to the consumer. For now, these differences and the level of importance ascribed to privacy rights and the protection, retention, and preservation of data can end up hindering efforts to obtain international consensus.\textsuperscript{35}

**IV. What Is Being Done to Address Cybercrime-Related Jurisdictional Concerns?**

**A. DOMESTIC INITIATIVES**

1. *Domestic Investigations*

One of the simplest ways domestic authorities can provide legal assistance to another jurisdiction is to determine if the conduct being investigated violates domestic law and, if so, open a domestic investigation. Opening a domestic investigation into the case allows authorities to cooperate on an informal basis, saving valuable time that would otherwise be spent waiting for the information to be funneled through the formal mutual legal assistance process.

2. *Cross-Border Searches*

Sometimes even expedited or informal procedures for obtaining international legal assistance may seem too time-consuming. When time is of the essence, authorities investigating cybercrime cases involving evidence stored on foreign servers may be tempted to conduct the search on their own rather than wait for formal assistance.

\textsuperscript{33}CoE Convention, Article 29.
\textsuperscript{34}See 18 U.S.C. Section 2703(f), the text of this provision can be found at http://www4.law.cornell.edu/uscode/18/2703.html.
from authorities in the foreign country. Such unilateral cross-border searches are controversial. They are often seen as potentially violating the sovereignty of the other nation. Critics also warn that conducting such cross-border searches could set a dangerous precedent. The concern is that it might lure other countries whose laws or interests are significantly different to search computers in another country for their own purposes, whether to gather evidence against one of its citizens in relation to conduct that is not illegal in the country where the computer resides or to conduct surreptitious searches of government or business computers for political or economic gain. Inadvertent cross-border searches can occur when an investigator downloads information that is stored on a server in another country. This occurs largely because the user is not aware of where a specific server is located.

So far, there has been at least one case in which law enforcement authorities have searched foreign computers without first obtaining the host nation’s express permission. The case, which is still before the courts in multiple states, involved the FBI searching a computer system in Russia that was operated by a group of Russian nationals suspected of being involved in cybercrime. The authorities in that case were looking for evidence in a string of hacking and extortion cases against American companies. The U.S. government had approached the Russian government on numerous occasions seeking assistance in the case, but without result. Unable to otherwise stop them, the FBI lured two suspects to the United States for a meeting with undercover agents. During the meeting, the suspects discussed breaking into U.S.-victim computer systems and extorting the operators of those systems. They also offered to demonstrate their hacking skills on a test computer system. In order to identify the suspects’ methods, a keystroke logger was used to capture the suspects’ activities on the undercover computers. At the end of the meeting, the suspects were arrested and the Russian consulate notified. When the undercover system logs were reviewed, investigators identified an account name and password used by the suspects during their hacking demonstration. With the suspects under arrest and the Russian consulate notified, the investigators sought to find out whether the system used by the defendants and their associates was still online. They discovered that it was. Concerned that the suspects’ associates could destroy the electronic evidence in an instant, the investigators contacted the prosecutors on the case and were directed to preserve data from the system in anticipation of applying for a search warrant. Following instructions from the prosecutors, the investigators accessed the Russian computer themselves, downloaded and sealed the data on
compact disks without reviewing it, and then applied to a U.S. court for a warrant authorizing its search and seizure.

In at least one of the cases, the accused moved to suppress the evidence. He argued, among other things, that the unilateral search violated search and seizure law in both Russia and the United States. The court denied the motion. It held that U.S. investigators were not bound by Russian search and seizure law, and that the protection against unreasonable search and seizure in the U.S. Constitution does not apply to a U.S. investigator’s extraterritorial access to computers in Russia or to their copying of data contained on them. The case remains controversial. The preferred route, of course, is to obtain legal assistance from foreign law enforcement through the appropriate channels; however, no international agreement exists over what actions a country may take when a foreign host nation is either unwilling or unable to provide effective law enforcement assistance.36

B. MULTILATERAL INITIATIVES

1. Council of Europe

(i) Introduction

On November 23, 2001, the first international treaty on computer and Internet-related crime was opened for signature in Budapest.37 The treaty, which is called the Convention on Cybercrime,38 was developed by the Council of Europe (CoE), culminating a five-year process dating back to early 1997. As of July 16, 2002, the Convention has been signed by 29 of the CoE’s Member States,39 along with CoE partner states: Canada, the United States, South Africa, and Japan.40 The Convention

---


37The Convention was adopted by the Council of Europe on Nov. 8, 2001.


39The 29 signatory members are: Albania, Armenia, Austria, Belgium, Bulgaria, Croatia, Cyprus, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Malta, Moldova, Netherlands, Norway, Poland, Portugal, Romania, Spain, Sweden, Switzerland, the Former Yugoslav Republic of Macedonia, the Ukraine, and the United Kingdom; http://conventions.coe.int/Treaty/EN/searchsig.asp?NT=185&CM=&DF.

40These four countries are not members of the CoE, but they participated in the drafting process.
will come into force when it is ratified by at least five countries, three of which must be CoE Member States.

The Convention consists of three main sections, addressing substantive law, procedural powers, and international cooperation. These sections aim to:

- Harmonize substantive criminal law by setting out the elements of various computer crimes and computer-related offenses;
- Assist law enforcement agencies in the investigation of cybercrime cases and cases involving electronic evidence; and
- Establish a rapid and effective system for international cooperation in relation to such cases.

While some of the other chapters describe aspects of the Convention in more detail, the following section focuses on how the Convention addresses cross-border or jurisdictional concerns.

(ii) Filling the Gaps in Substantive Criminal Laws and Harmonizing Elements of Cybercrime Offenses

As noted earlier, one of the biggest challenges in investigating and prosecuting international cybercrime cases is the dilemma that the conduct in question may not be illegal under some countries’ criminal laws. Moreover, among countries that already have computer-specific criminal laws, inconsistencies in approaches, definitions, and sanctions can hinder international cooperation, particularly when it comes to assistance.

The CoE Convention addresses these concerns by first creating a minimum list of offenses and, second, attempting to harmonize the elements of those offenses. In doing so, the CoE Convention strikes a delicate balance. On the one hand, it requires signatories to ensure that their domestic laws are capable of covering these offenses; on the other, it provides enough flexibility to allow individual countries to modify the offenses as required by allowing them to establish more stringent standards or opt out of certain provisions altogether.

In terms of the specifics, the CoE Convention addresses:

- Offenses against the confidentiality, integrity, and availability of computer data and systems;\(^{41}\)
- Computer-related offenses (forgery and fraud);\(^{42}\)

---

\(^{41}\)These consist of the offenses of illegal access (Article 2), illegal interception (Article 3), data interference (Article 4), system interference (Article 5), and misuse of devices (Article 6).

\(^{42}\)Computer-related forgery is addressed in Article 7; computer-related fraud in Article 8.
Content-related offenses (presently limited to the production, dissemination, and possession of child pornography),\textsuperscript{43} and
- Offenses related to infringement of copyright and related rights through the unauthorized reproduction and dissemination of protected works over the Internet.\textsuperscript{44}

These represent a minimum consensus and do not preclude extensions under domestic law.\textsuperscript{45} The treaty also requires that domestic laws cover attempts at, or the aiding and abetting of, these offenses, and that they be broad enough to hold legal persons liable for the offenses set forth above.\textsuperscript{46}

By harmonizing substantive criminal laws, at least among the countries that sign onto the treaty, the CoE Convention will contribute toward the development of an international framework that can ultimately guide other countries around the world. At the same time, by filling gaps in the international patchwork of cybercrime laws, it may help avoid repeats like the outcome of the I LOVE YOU virus case and empower investigating countries to bring such cases to trial.

(iii) Improving Law Enforcement’s Ability to Investigate Cybercrime

To ensure that parties to the CoE Convention are capable of responding promptly and effectively to such mutual assistance requests, the CoE Convention establishes an international 24/7 Point of Contact Network and requires each signatory to designate a point of contact to be available on a 24-hour/7-day-a-week basis. Among other things, the points of contact are to provide assistance with the preservation of data, the collection of evidence, the provision of legal information and technical advice, and the location of suspects.\textsuperscript{47}

\textsuperscript{43}The child-pornography offenses are addressed in Article 9. While certain countries asked that the Convention’s content-related category be expanded to include hate speech as well, the drafters were unable to obtain consensus. As a result, hate speech was not included in the body of the Convention. It is to be added, however, to a protocol to the Convention, which is to cover the propagation of racist and xenophobic ideas over the web. A preliminary draft of the protocol, dated Mar. 26, 2002, is available from the Council of Europe’s website at http://conventions.coe.int/treaty/EN/cadreprojets.htm.
\textsuperscript{44}Copyright and related rights are addressed in Article 10.
\textsuperscript{45}In each case, for conduct to qualify as an offense, two conditions must be met: (1) the offense must be committed intentionally; and (2) it must be committed “without right”; that is, the conduct described is not always punishable per se, but may be justified by law, regulations, a legally binding contract, or a justificatory fact.
\textsuperscript{46}CoE Convention, Article 11.
\textsuperscript{47}CoE Convention, Article 35.
If one country asks another to preserve communications data pending a request for further assistance, the foreign law enforcement agency may not be able to do so if it does not have legal authority to preserve such evidence in its own investigations. Put another way, a foreign law enforcement agency can only do what it is empowered to do under its own laws.

The CoE Convention addresses these concerns by seeking to ensure that law enforcement has the investigative powers necessary to cooperate in cybercrime cases. In doing so, it helps ensure prompt and effective legal assistance from countries that are party to the treaty. To touch briefly on the procedural powers, the Convention creates four categories of powers and procedures:

- The expedited preservation of stored computer data;
- Production orders;
- The search and seizure of stored computer data; and
- The real-time collection of traffic data.

A point worth noting is that the Convention's procedural provisions are not limited to cybercrime cases. The procedural powers apply to investigations of the offenses established under the Convention and to other criminal offenses committed by means of a computer system, but they also extend to collection of electronic evidence in any criminal case, even if the offense it relates to is not computer-related.

Under Article 16, signatories must enable their "competent authorities" to "order or similarly obtain" the expeditious preservation of specified computer data to keep it safe from modification, deterioration, or deletion for as long as necessary, up to a maximum of 90 days. Article 17 establishes specific obligations in relation to the preservation of traffic data and provides for expeditious disclosure of a sufficient amount of traffic data to identify the service providers that were involved in the transmissions.

Under Article 18, signatories must enable their competent authorities to compel people located in their territories to produce specified computer data in their possession or control. They must also be able to compel service providers offering services in their territories to produce subscriber information in their possession or control.

Article 19 requires signatories to empower their competent authorities to search computer systems in their territories, along with computer data stored in those systems or on another storage medium. The authorities must be allowed to extend the search to another computer system if they have grounds to believe the data they are seeking is stored in another computer system or is accessible from the initial system. They must also be empowered to seize a computer system or a computer data storage medium, to make and retain a copy of the computer data, and to render it accessible or remove it from the accessed system.

Article 20 provides for the real-time collection of traffic data, while Article 21 provides for the real-time interception of content data. Because of the privacy concerns raised by the interception of content data and the invasiveness of the measure, the Convention prescribes that the measure is only available in relation to serious offenses (to be determined by domestic law).
To guard against potential abuses in the exercise of such powers, the Convention requires that the signatories incorporate the principle of proportionality and that the powers be exercised in a way that does not violate human rights.53

(iv) Establishing Jurisdiction and Avoiding Gaps
To ensure that cases do not fall through the cracks when, for example, no country claims jurisdiction over a case, the Convention requires signatories to establish criminal jurisdiction over offenses in certain situations. Among other things, signatories must establish criminal jurisdiction over offenses committed “in their territory.”54 While this is helpful, it may nevertheless be difficult to determine when an offense involving data on computer networks occurs “in” a country’s territory. Fortunately, the Convention also addresses the scenario of an offense committed “outside the territorial jurisdiction of any State.” This would presumably encompass crimes that no signatory country determined occurred in its territory, in which case the Convention perhaps would apply as though the offense were committed in a country not a signatory to the Convention. In such cases, if the offender were a national of any of the countries party to the treaty (even though the offense was committed in a nonparty country), that country would be required, under the provisions of the Convention, to establish criminal jurisdiction over the offense.

(v) Establishing Jurisdiction: Consulting with Other Countries That Have an Interest in the Case
The Convention allows each country to pursue a case on its own, provided it can establish jurisdiction. It may be counterproductive, however, for each country to proceed in isolation; the better route is consultation and cooperation. As noted in Part III of this chapter, a computer-related crime may implicate several countries at the same time. Evidence or victims may be scattered across a number of countries,

53CoE Convention, Article 15. According to paragraph 146 of the Explanatory Report on the CoE Convention, proportionality is meant to be implemented according to the relevant principles of domestic law of each signatory state. For European countries, this shall be according to the principles of the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms. It is intended that other states apply related principles, such as limitations on production orders and reasonableness requirements for searches and seizures.
54CoE Convention, Article 22. This Article provides for substantial reservation possibilities for countries that do not universally assume jurisdiction over its nationals overseas or on certain transportation modes.
producing more than one country with an interest in investigating or prosecuting the case.

The CoE Convention addresses this precise issue by expressly requiring consultation. When more than one signatory claims jurisdiction over an offense, the Convention requires them to consult with a view to determining the most appropriate jurisdiction for prosecution.

(vi) Providing for Extradition
If a country wishing to prosecute a case wants to extradite the suspect but does not have a relevant extradition treaty in place, it ordinarily would have no formal vehicle for requesting the suspect’s extradition. If the country from which extradition is sought extradites only to countries with which it has a treaty, it would likely refuse to voluntarily hand over the suspect, making it impossible for the investigating country to prosecute the case—unless the suspect voluntarily agrees. If the country does not make extradition contingent on the existence of an extradition treaty, its decision would nevertheless be discretionary. It could agree, but it could just as easily refuse.

Ordinarily this would bring the case to an end. Under the CoE Convention, if such countries are both parties to the Convention, and if the one from whom extradition is sought requires that there be a treaty, it may consider the Convention as the legal basis for extradition with respect to any criminal offense referred to in the Convention. If, on the other hand, the country asked to turn over the suspect(s) does not make extradition conditional on the existence of a treaty, the Convention would require that it recognize the criminal offenses referred to in the Convention as extraditable offenses between them.55

Extraditable offenses can also be a point of concern for countries that do have treaties in place. If hacking, for example, is not an extraditable offense in an extradition treaty between two given countries, the country asked to extradite a suspected hacker, pursuant to the treaty, would not be obliged to do so. The CoE Convention, however, addresses this point by making all the offenses described in the Convention extraditable offenses. The Convention’s offenses are not only deemed to be extraditable offenses for the purpose of any existing extradition treaty between or among the parties; they must also be included as extraditable offenses in any future treaties negotiated between them.

(vii) Providing for Mutual Assistance
The CoE Convention is particularly helpful in clarifying rights and obligations in relation to mutual assistance. It requires, first and foremost, that parties to the Convention provide mutual assistance

55CoE Convention, Article 24.
“to the widest extent possible.”\textsuperscript{56} In terms of specifics, the Convention provides for mutual assistance with respect to:

- The access of stored computer data,\textsuperscript{57}
- The real-time collection of traffic data,\textsuperscript{58} and
- The real-time collection or recording of content data.\textsuperscript{59}

It also recognizes the transient and vulnerable nature of electronic evidence by establishing a framework for expedited legal assistance. Among other things, the Convention enables one party to request that another party:

- Expeditiously preserve stored computer data pending a further request for assistance;\textsuperscript{60}
- Expeditiously disclose sufficient amounts of the preserved traffic data to identify the service provider involved in the transmission;\textsuperscript{61} and
- Require parties to respond on an expedited basis to mutual-assistance requests regarding access to stored computer data where there are grounds to believe that relevant data are particularly vulnerable to loss or modification.\textsuperscript{62}

2. Group of Eight (G-8)

(i) Background

The G-8 is an international multilateral group consisting of Canada, France, Germany, Italy, Japan, Russia, the United Kingdom, and the United States.\textsuperscript{63} While the group was founded as an informal forum for

\textsuperscript{56}CoE Convention, Article 23.
\textsuperscript{57}CoE Convention, Article 31.
\textsuperscript{58}CoE Convention, Article 33.
\textsuperscript{59}CoE Convention, Article 34.
\textsuperscript{60}CoE Convention, Article 29.
\textsuperscript{61}CoE Convention, Article 30.
\textsuperscript{62}CoE Convention, Article 31.
\textsuperscript{63}The Group originated in 1975 at an Economic Summit convened by President Valery Giscard d’Estaing of France and attended by leaders from Germany, Japan, the United Kingdom and the United States. President Giscard and Chancellor Schmidt of Germany wanted to establish an informal forum for world leaders to discuss world economic issues. Italy and Canada joined this original “Group of Five” in 1976–77 and the configuration became known as the Group of Seven, or “G-7.” At that time, G-7 meetings followed a limited agenda of economic issues, and were intended to provide an informal consultation forum. In the 1980s, these annual meetings became more formalized, with an agreed statement, or “Communiqué,” issued by the leaders at the conclusion of each summit, and Heads of State expanded the agenda beyond economic issues. At the end of the cold war, as democratic and economic reform got underway in Russia, Russian leaders were gradually integrated into the G-7 and, in 1998, the group’s name was formally changed to the “G-8.”
world leaders to discuss economic issues, the agenda has expanded to include other global issues, including transnational crime. The discussions take place once a year at annual summits, with the heads of state issuing an agreed statement, or communiqué, at the end of each summit.

After the 1995 G-8 Summit in Halifax, Nova Scotia, a group of experts known as the Lyon Group was assembled to look for better ways to fight international crime. In 1996, the Lyon Group produced 40 recommendations to combat transnational organized crime. These recommendations were endorsed by the heads of state at the G-8’s summit in June of that same year (Lyon Summit).

One of the recommendations endorsed at the 1996 Lyon Summit dealt specifically with high-tech crime and, among other things, jurisdiction. Recommendation 16 called for countries to “review their laws in order to ensure that abuses of modern technology that are deserving of criminal sanctions are criminalized and that problems with respect to jurisdiction, enforcement powers, investigation, training, crime prevention and international cooperation in respect of such abuses are effectively addressed.” The G-8 has continued to make high-tech crime a high priority.

(ii) G-8 Subgroup on High-Tech Crime
To implement Recommendation 16 and otherwise enhance law enforcement’s ability to combat high-tech and computer-related crime,

---

64See “P8–Senior Experts Group Recommendations,” Senior Experts on Transnational Organized Crime, Apr. 12, 1996, http://ue.eu.int/ejn/data/vol_c/9_autres_textes/40rag7en.html. The referenced document refers to the P8, which is the Group of Seven nations plus Russia.

65In February 2002, the G-8 considered, but did not adopt, the following nine non-binding principles for enhancing security: (1) Countries should create emergency watch and warning networks to quickly inform agencies and the public about impending attacks or viruses; (2) Industry, government, and the private sector should share appropriate critical infrastructure information; (3) Legal systems must ensure that industry, government, and the private sector are, in fact, able to share critical infrastructure information, when appropriate; (4) Legal systems and law enforcement personnel must facilitate prompt passing of data to other countries, when appropriate; (5) Countries should work to create secure and stable government communications for emergency situations; (6) Countries should map their critical infrastructures and identify infrastructure interdependencies; (7) Legal systems must ensure that laws regarding data destruction preservation and disclosure protect their own infrastructure as well as aid other countries in protecting infrastructure; (8) Work in this area should be coordinated among all stakeholders; and (9) Countries should conduct training or exercises to enhance their response capabilities.
the Lyon Group formed a Subgroup in January 1997 called the G-8 Subgroup on High-Tech Crime. The Subgroup held five meetings that year, and has been meeting regularly since. The work of the Subgroup has remained focused on enhancing the abilities of law enforcement to prevent, investigate, and prosecute high-tech and computer-related crime. Among other things, the Subgroup has:

- Established an international network of 24-hour high-tech points of contact.
- Reviewed and assessed the G-8 legal systems as they relate to combating cybercrime.
- Considered principles concerning transborder access to stored data.
- Developed computer forensic principles for circumstances where digital evidence retrieved in one country requires authentication in the courts of another country.
- Agreed to comply with transborder data preservation requests.
- Standardized law enforcement requests to industry.
- Agreed on recommendations for tracing terrorist and criminal communications across borders.

(iii) Principles and Action Plan

In December 1997, U.S. Attorney General Janet Reno hosted the first-ever meeting of her G-8 counterparts: the Justice and Interior Ministers of the G-8’s member countries. The meeting focused on computer crime. At the end of the meeting, the ministers adopted ten principles and a ten-point action plan to combat high-tech crime.66

Action Item One from the 1997 Communiqué called for creation of an international network of high-tech-crime points of contact from law enforcement that can be reached 24 hours a day, 7 days a week for urgent requests for assistance. From an initial membership of just the G-8 countries, the network presently includes approximately 30 countries, with recruitment ongoing.

At a subsequent meeting in Moscow in October 1999, the G-8 Justice and Interior Ministers acknowledged the importance of sharing information, not just among Member States, but with private industry as well. To this end, the ministers directed their officials to “convene a

---

conference where the G-8 and industry can share ideas on Internet crime, with particular emphasis on issues relating to locating and identifying Internet criminals." Three such conferences followed: in Paris (May 2000), Berlin (October 2000), and Tokyo (May 2001). Government/industry workshops at the conferences addressed issues such as data preservation, data retention, real-time tracing, threat assessment and prevention, protection of e-commerce, and training.

3. Organization of American States

In March 1999, the Attorneys General and Ministers of Justice and Interior of the Organization of American States (OAS) recommended the establishment of an intergovernmental experts' group on cybercrime. The group's mandate was to: (1) study crime targeting computers and information in the Member States; (2) assess national legislation, policies, and practices applicable to such crime; (3) identify national and international entities with relevant expertise; and (4) identify mechanisms of cooperation within the inter-American system to combat cybercrime.

To this end, the first meeting of OAS experts on cybercrime convened in May 1999. The group of experts crafted a survey asking Member States about:

- Their experience with various types of cybercrime;
- The substantive laws governing cybercrime;
- The jurisdiction and extradition principles governing cybercrime;
- The laws governing the preservation and gathering of evidence in such cases; and
- The existence of specialized training programs or law enforcement entities and/or experts to combat cybercrime.

The survey results were analyzed at a second meeting in October 1999 with a view to determining how member countries can cooperate on issues related to cybercrime. The findings led to a series of

---

68The members of the Organization of American States are: Argentina, Bolivia, Brazil, Chile, Colombia, Costa Rica, Cuba, the Dominican Republic, Ecuador, El Salvador, Guatemala, Haiti, Honduras, Mexico, Nicaragua, Panama, Paraguay, Peru, the United States, Uruguay, Venezuela, Barbados, Trinidad and Tobago, Jamaica, Grenada, Suriname, Dominica, Saint Lucia, Antigua and Barbuda, Saint Vincent and the Grenadines, the Bahamas, St. Kitts and Nevis, Canada, Belize, and Guyana. See http://www.oas.org.
recommendations designed to help Member States better respond to the challenges and public security concerns created by new technologies. These recommendations were presented in a final report.69

4. European Union

The European Commission launched the eEurope initiative in December 1999 following the Tampere European Council70 and, in June 2000, the Feira European Council adopted a comprehensive eEurope Action Plan to be implemented before the end of 2002.71 The European Commission has made meeting this goal and establishing a European computer crime observatory a priority. The planned observatory would be established within Europol, the European Police Office, and is required to promote effective investigation and prosecution methods throughout the Member States, among other responsibilities.

The EU Forum on Cybercrime provides a platform for discussion and cooperation between law enforcement agencies, Internet Service Providers, telecommunications operators, civil liberties organizations, consumer representatives, data protection authorities, and other interested parties. It was established following the 2000 publication of the Communication of the European Commission “Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime.”72

Subsequently, in a Communication from the Commission of the European Communities to the Council, the European Parliament, the European Economic and Social Committee, and the Committee of the Regions regarding network and information security, the Commission lists several methods for improving coordination among

---

the European states with respect to cybercrime prevention and enforcement. The proposed measures include:

- Launching a public awareness campaign.
- Strengthening Member States’ Computer Emergency Response Teams and improving coordination among the teams.
- Supporting research and development in security.
- Supporting market-oriented standardization and certification.
- Proposing cybercrime legislation and supporting free distribution of encryption products.
- Reinforcing dialogue on information security.\textsuperscript{73}

The most recent initiative of the European Commission is the Proposal for a Council Framework Decision on attacks against information systems released in April 2002. In this document, the European Commission declares that attacks against information systems constitute a threat to the achievement of a safer Information Society and the EU goal of an “Area of Freedom, Security, and Justice.”\textsuperscript{74} The Commission’s proposal calls for the harmonization of Member States’ criminal laws regarding attacks against information systems. This will improve cooperation by ensuring that the dual criminality requirement is fulfilled for mutual legal assistance, and the planned observatory will provide attack assistance to all countries.

C. INTERJURISDICTIONAL NETWORKS AND OTHER INITIATIVES

Cybercrime is a global problem, and, fortunately, there is a wealth of resources and models to draw upon for countries that need assistance. Many of the gains in fighting crimes that span international borders come from international networks and informal initiatives set up to provide international assistance. Countries that need assistance in dealing with these issues, either at a legal or practical level, can take advantage of such networks or learn from these models. A number of such initiatives are set out below.


1. U.S. Customs Service Cyber Smuggling Center

As investigation and enforcement in cybercrime cases are quickly becoming a law enforcement priority, national law enforcement agencies in the United States have undertaken to cooperate informally with foreign law enforcement agencies in various areas. One of the most active U.S. agencies in this drive toward informal cooperation is the U.S. Customs Service, which established a Cyber Smuggling Center in August of 1997. The Cyber Smuggling Center develops leads, tips, and complaints for several types of crimes, some of which are described below.\(^75\) Several of the initiatives include the following:

(i) Child Pornography

In the area of child pornography, the Cyber Smuggling Center conducts undercover operations to identify child-pornography producers and distributors at the international level. Since 1997, the Customs Service has jointly investigated child pornography with several foreign nations. A joint initiative with the German federal police, known as “Operation Kinderschutz,” led to the arrest of a Maryland resident. Customs agents have also worked with British, Russian, and other foreign officials on child pornography investigations.

(ii) Pharmaceuticals

The Cyber Smuggling Center has also informally cooperated with foreign countries regarding the unlawful distribution of pharmaceuticals. While the Internet is a growing legitimate source of prescription drugs, some online pharmacies flout domestic law. Under the U.S. Food, Drug, and Cosmetic Act (FDCA), prescription drugs may be dispensed only with a valid prescription from a practitioner properly licensed to administer the drug.\(^76\) Some non-U.S. websites, however, are selling prescription drugs; these drugs are then illegally imported into the United States. The Cyber Smuggling Center has been working with U.S. Customs attaché offices and their foreign counterparts to identify these non-U.S. sites. Once the U.S. Food and Drug Administration determines that the drugs sold by these sites violate the FDCA, Customs’ International Mail Facilities will stop and seize parcels entering the United States.

---

\(^{75}\) For further information, see the Customs CyberSmuggling Center’s website at http://www.customs.ustreas.gov/enforcem/cyber.htm.

(iii) Intellectual Property Violations

A third, and perhaps more controversial area of the U.S. Customs Service’s Cyber smuggling operations is intellectual property violations. The Cyber Smuggling Center has been working closely with industry representatives and has investigated distributors in Russia, Malaysia, Singapore, and the United Kingdom regarding commercial quantities of pirated U.S. merchandise sold to customers over the Internet. The pirated merchandise includes business software, video games, movies, and sound recordings. Recently, the Cyber Smuggling Center coordinated enforcement actions against computer software copyright infringement with Australia, England, Norway, Finland, and Sweden in an operation called “Operation Buccaneer.”

2. International Marketing Supervision Network

The International Marketing Supervision Network (IMSN) is an organization of consumer protection law enforcement agencies from more than two dozen countries. The IMSN’s mandate is to share information about cross-border commercial activities that may affect consumer interests and to promote international cooperation on consumer protection issues. In 1997, for example, the U.S. Federal Trade Commission, which is the U.S. representative to the IMSN, targeted an Internet domain name scam operating out of Australia. The FTC alerted its Australian IMSN counterpart, leading to an Australian enforcement action. In another Internet fraud case in 1999, the FTC worked with its Portuguese IMSN counterpart to tackle an Internet scam involving pornographic material.

3. International Task Forces

U.S. consumer protection agencies have also established less formal international task forces to address cross-border consumer fraud, such as

77In 1999, the Customs Service and the Department of Justice (including the FBI) announced an initiative aimed more generally at intellectual property violations. Internationally, the initiative pledges support from the DOJ and FBI for the efforts of the Department of State, the Customs Service, and trade agencies with intellectual property expertise. The initiative also seeks to help U.S. trading partners enforce intellectual property laws. The National Intellectual Property Law Enforcement Coordination Council, established in 1999, also seeks to coordinate domestic and international intellectual property law enforcement matters among federal and foreign entities.

78The website of the IMSN is at http://www.imsnricc.org/.

79As part of its activities, the IMSN conducts “Internet sweeps,” in which participating law enforcement agencies surf the Internet looking for “fraudulent and deceptive scams.” For more information, refer to the discussion of Internet sweeps at the IMSN website at http://www.imsnricc.org/imsn/activities.htm.
as the U.S.–Canada Telemarketing Fraud Task Force and the Mexico–U.S.–Canada Health Care Fraud Task Force.

4. Memoranda of Understanding (MOUs)

The U.S. Securities and Exchange Commission (SEC) has formulated a unique solution to jurisdictional issues in its criminal investigations. The SEC negotiates bilateral agreements with foreign counterparts to facilitate cooperation in investigations. These agreements, called Memoranda of Understanding (MOUs), are nonbinding agreements between the SEC and its foreign counterparts. There is no law that authorizes such agreements. They are privately negotiated and are not ratified by the U.S. Senate, as a treaty would be.

Nevertheless, MOUs are widely used for international cooperation, and the SEC has entered into over 30 such agreements as of 1999. The advantage of MOUs is that they are bilateral in nature, making it possible to customize each agreement to achieve the greatest level of cooperation even when the respective markets and regulatory powers of the countries involved are quite different.

5. Executive Agreements

In some circumstances, law enforcement can avoid jurisdictional hurdles in gathering foreign evidence by resorting to an executive agreement. The United States and Columbia, for example, have entered into an executive agreement that addresses the sharing of evidence in certain cases. The United States has also entered into such agreements in the areas of tax and customs. Agreements like these conceivably could be expanded to extend to cybercrime cases, providing valuable assistance with jurisdictional issues—especially where no formal procedure for mutual legal assistance is in place.

6. Interpol

Interpol is an international law enforcement organization whose goal is to “provide a unique range of essential services for the law enforcement community to optimize the international effort to combat crime.” As part of its mandate, Interpol has created several regional

---

82See the section entitled “Interpol Information” at http://www.interpol.int.
working parties on information technology crime. Each working party is a group of experts gathered from the national computer crime units of the countries in designated regions. While they are all at different stages of development, the European Working Party is the most active and serves as a model for the others. The European Working Party has, among other things, developed resources for both novice and experienced cybercrime investigators. It has, for example, prepared a handbook on the investigation of computer-related crime, which serves as an introduction for the novice cyber investigator. The working party has also developed a computer crime manual outlining best practices for the experienced investigator. The manual, which is continually updated, is available on CD-ROM and is being converted to HTML format so that it can be made available through the Interpol website. With resources such as these and participation from 179 member countries from around the world, Interpol is clearly positioned to provide valuable assistance to countries needing help in their efforts to combat cybercrime.

7. International Chamber of Commerce

The International Chamber of Commerce (ICC) has established a special unit to build a database on criminal methods in cyber space and to act as an interface between law enforcement and the private sector. With associations with over 130 companies, the ICC is well positioned to gather and organize groups to exchange information and discuss possible action plans.

8. World Information Technology and Services Alliance

The World Information Technology and Services Alliance is a consortium of 41 information technology industry associations from around the world. It is dedicated, in part, to sharing information

---

83For further information on the working parties, see http://www.interpol.int/Public/TechnologyCrime/WorkingParties/default.asp.
84See www.interpol.int.
85According to its website, the ICC Cybercrime Unit keeps track of criminal methods, briefs its members, provides expert advice on the security of information systems, identifies criminal interference in corporate computer networks, work closely with national and international law enforcement agencies, and constitutes a prime source of information, research, and intelligence: http://www.iccwbo.org/ccs/menu_cybercrime_unit.asp.
86The organization's website is at http://www.witsa.org/.
and building partnerships across economic sectors by hosting Global Information Security Summits that bring together industry, governments, and multilateral organizations.

9. Business Software Alliance

The Business Software Alliance (BSA) is an organization devoted to combating intellectual property crimes. Its membership includes companies such as Adobe, Apple Computer, Microsoft, Novell, Sybase, Symantec, and Unigraphics Solutions. BSA has also launched the Assistance in Software Auditing Program, which is designed to ensure that organizations use only licensed software.87

10. Information Sharing and Analysis Centers (ISACs)

Around the world, various industries have been establishing Information Sharing and Analysis Centers (ISACs) to share real-time information about threats, vulnerabilities, attacks, and countermeasures.88 ISACs are not new, but they are relatively new to the technology sector. Despite the obvious privacy and conflict-of-interest issues involved in sharing such information across an industry sector, a number of large technology companies banded together in 2001 to create an information technology ISAC, and global business organizations have recently broadened their respective mandates to include the delivery of commercial crime prevention services to its members. According to Harris Miller, president of the Information Technology Association of America, “The hope is to catch these problems earlier and try to stop things before they happen rather than mitigate them.”

The 19 technology companies that formed the ISAC—including AT&T, Cisco, Hewlett-Packard, Microsoft, and Oracle—did so as a private alliance to share sensitive information about cyber attacks and vulnerabilities in their software and hardware products. Members that discover a new cyber threat are able to send detailed warnings to the rest of the group, and the group will determine how much of that information to share with other industries or the U.S. government.

Ideally, the ISACs and the government should engage in a two-way sharing of information. Under this model, the government would contact the ISACs to share information on threats, vulnerabilities, orchestrated

---

87 The organization’s website is at http://www.bsa.org.
88 The banking, telephone, and electrical industries, for example, have each banded together to establish industry-specific ISACs.
attacks, assessment services, and network security products, and in turn, would anticipate that the ISACs provide the same information from the private sector to the appropriate government agencies. Such a public/private initiative would optimally provide cost-effective opportunities for a private business to use federal government resources while maintaining control over the investigation of disruption of service and other computer crimes.

11. Academia and Think Tanks

Academia has also been active in addressing jurisdictional issues related to cybercrime. As an example, in December 1999, a number of U.S. research and educational institutions sponsored a conference that yielded the August 2000 Stanford Draft International Convention to Enhance Protection from Cyber Crime and Terrorism (Stanford Draft).89 The Stanford Draft proposes the establishment of an international Agency for Information Infrastructure Protection (AIIP) to serve as a formal structure in which interested groups would cooperate through experts in developing cyber security standards and practices. It also addresses some of the jurisdictional issues raised elsewhere in this chapter. In fact, the purpose of the draft was to resolve certain issues more definitively than what had been included in the draft Council of Europe Convention on Cybercrime (CoE draft) at that time.

For instance, the CoE draft enumerated the instances in which parties would be obliged to establish jurisdiction over the Convention’s offenses. It did not resolve potential jurisdictional conflicts but merely directed party States to consult with one another.90 The Stanford Draft, on the other hand, anticipates that jurisdiction could potentially exist in multiple states for the same offense, and establishes a set of priority rules for resolving jurisdictional conflicts.

It provides, first, that prescriptive and enforcement jurisdiction exists in states: (1) in which offenses are committed; (2) in which alleged offenders are citizens, reside, or are present; or (3) in which the


90The draft contained the same wording that was ultimately incorporated into the final Convention. It required that parties “where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.”
conduct of offenders has substantial effects. Under Article 5 of the Stanford Draft, a state would be required to establish jurisdiction in these situations. A state would also be entitled to establish jurisdiction over offenses covered by the draft when (a) they are committed with the intent or purpose (i) to harm the State or its nationals or (ii) to compel the State to do or abstain from doing any act; or (b) the offenses have substantial effects in the state. Priority in jurisdiction would then be established in the following order: (1) in which the alleged offender was physically present when the alleged offense occurred, (2) in which substantial harm was suffered, (3) in the state of the alleged offender’s dominant nationality, (4) in which the alleged offender was found, and (5) any place “with a reasonable basis for jurisdiction.” Moreover, the draft requires all states in which an alleged offender is present to either prosecute or extradite.

To minimize the jurisdictional conflicts inherent in addressing cybercrime, enforcement under the Stanford Draft is limited to “universally condemned” conduct. The Stanford Draft does not accede to a state’s jurisdiction merely because someone within its territory is able to access a website in another state. To confer jurisdiction, someone in control of the website must deliberately cause one of the covered crimes, with effects in the state seeking to assert jurisdiction.

As the Stanford Draft shows, academia and research centers can be a valuable resource in recommending solutions and approaches to areas of concern. In short, the more we bring such issues to the forefront and the more we encourage public discussion and debate, the better prepared we will be to tackle such challenges. No single agency or country can do it alone.

V. Conclusion

When jurisdictional issues occur, particularly in cybercrime cases, they depend on cooperation from all countries and the legal systems involved. Law enforcement entities in particular must be able to work together, often on an expedited basis. They must have the capacity, for example, to respond promptly to requests for assistance with the interception, preservation, or search and seizure of electronic data. Legislators must ensure there are adequate laws capable of capturing computer-related offenses, and the courts must grapple with sometimes difficult scenarios involving conflicting or inconsistent laws among the countries involved.

A number of international initiatives have attempted to address cross-border jurisdictional concerns. The most significant is the CoE
Convention on Cybercrime. There is also a wealth of resources, models, and networks available to assist countries. However, there remains a serious lack of international coordination and consensus on these important issues. Clearly, cybercrime is a global problem that calls for a global solution.
CHAPTER ❖ 3

Law Enforcement

I. Introduction

A. THE IMPACT OF THE GLOBAL INTERNET ON LAW ENFORCEMENT

Since the early 1990s, the global information and communication technology (ICT) industry sector began an important transformation by adopting Internet Protocol (IP) based technologies as its core networking technology. These packet switching technologies, combined with the rapid rate of technological advancement and growth of the Internet, have presented law enforcement around the globe with new, complex challenges. Consider, for example, the June 2002 Netcraft survey indicating there were as many as 38 million instances of web server software installed on computers connected to the global Internet.\(^1\) Just ten years ago, there were essentially none. Even sophisticated law enforcement teams have trouble keeping up with this rate of growth; many developing countries view their ability to keep pace as hopeless.

Additionally, the modern-day enterprise has run up against the harsh reality that the Internet is inherently insecure. That the vast majority of personal computers connected to the Internet use operating systems that were never designed with security as a priority, compounds the problem. The periodic damage and losses incurred from viruses and various distributed denial-of-service attacks serve as serious reminders of information and infrastructure vulnerabilities and highlight shortcomings in the law enforcement arena. According to the


81
2002 CSI/FBI Computer Crime and Security Survey of computer crime in the United States, respondents' estimated total annual losses associated with computer crime have risen over the years, with 223 respondents reporting losses of US$456 million in the year 2002 alone. Total losses reported by survey participants over the six-year period of 1997 to 2002 amount to nearly US$1.5 billion. The threat, however, is global. The Economic Crime Survey 2001 of 536 European companies by PriceWaterhouseCoopers found that 43 percent of companies saw cybercrime becoming the biggest risk in the future. Similar concerns are voiced by Asian-Pacific Rim economies and other parts of the world.

The emergence and rapid escalation of cybercrime has important implications for governments and citizens all over the world. It demands ongoing government attention and resources devoted to high-tech investigative and forensic training, the establishment of internal organizations, and active involvement on the international front. It also calls for a new partnership between the public and private sectors to enhance the ability of law enforcement to meet the challenge of high-tech crime. Such a partnership should be based on information sharing, cooperation, and joint work toward fostering global minimum standards.

B. REDEFINING LAW ENFORCEMENT

"If crime crosses all borders, so must law and order."
Kofi A. Annan, Secretary-General, United Nations

Whenever enterprises have opened their doors for business, they have found that in addition to attracting customers they have also attracted criminals. This is not new, and over the centuries, nations have established laws, courts, and police to detect, deter, and punish crime. However, before the Internet became widespread, societies generally dealt with crime that was local in nature. That is, the scene of the crime was local and the criminals and victims were typically to be found in the general vicinity of the crime or fleeing from it. Furthermore, the law enforcement organization called in to apprehend the criminals,

---

and the courts that had legal jurisdiction, were usually local as well, or at least within the same state or province.

The Internet and the rapid deployment of ICTs in recent years have changed this historic trend. Today, the Internet revolution has created a tremendous challenge for law enforcement to develop the capacity to confront transnational crimes and follow trails of evidence—in real-time. The international bodies and laws that have been established to address issues concerning international trade also face new problems, and countries around the world realize they must change their laws to accommodate a global, developing legal framework regarding the use of ICTs, cybercrime, and the needs of law enforcement.

Computers can be engaged in cyber criminal activities in three ways:

1. They can be the target of an offense. This occurs when the confidentiality, integrity, and availability of data and/or networks are compromised. Viruses, denial-of-service attacks, and the theft or sabotage of data fall within this category.

2. They can be the tool used to commit a crime. This includes criminal activities facilitated by ICTs, such as fraud, child pornography, the sale of illegal substances online, or even murder or rape.

3. They can be incidental to a crime but have significant importance to law enforcement, such as when evidence concerning criminal activities is stored on computers and servers.

In addressing these kinds of activities, challenges are presented on three fronts:

1. Technical challenges are caused by (a) rapid changes in technology and the inability of law enforcement to stay current, and (b) technical shortcomings that impair finding and prosecuting cyber criminals.

2. Legal challenges are caused by procedural barriers or hurdles and the inability of legal frameworks around the globe to keep up with technological capabilities and the changing business environment.

3. Operational challenges are caused by (a) a lack of equipment and training and adequate organizational structures, and (b) the need to work with great speed within time zone, language, and cultural differences.5

---

The modern-day criminal can use a computer connected to the Internet and engage in criminal activities in any country around the world without the need for visas, passports, or airline tickets. The communications associated with such acts can flow through many countries and computers, and the critical evidence can be stored on servers in countries other than where the criminal is located. Victims can be scattered around the globe. The investigation of these activities necessarily involves law enforcement, lawyers, prosecutors, and government officials from every affected country plus international police organizations, such as Europol and Interpol. Criminals realize that this scenario poses tremendous hurdles to the effective investigation and handling of these crimes. Therefore, they are rapidly developing sophisticated technical expertise and learning how to use advanced technologies, such as encryption, anonymity, and steganography software to facilitate their cyber criminal activities.

C. CHAPTER OVERVIEW

This chapter discusses the impact of rapidly escalating high-tech crime on law enforcement and highlights the problems encountered in international investigations and cooperation between law enforcement officials. Part II discusses the current state of affairs and priority issues regarding cybercrime, what can be done on a national level, and international law enforcement initiatives. Part III addresses the practical investigatory consideration facing law enforcement today and highlights immediate needs.

II. Impact of Cybercrime on Law Enforcement

A. ICTs BRING A NEW WORLD

At the International Computer Crime Conference held in Oslo, Norway in May 2000, a former U.S. government official noted:

While the Internet may be borderless, national boundaries exist for law enforcement and we must respect the sovereignty of each

---


7Steganography is often accomplished by using a software program to hide data, pictures, or text within another document or image, where it is invisible to the eye and undetected by firewalls. Special software is needed to detect data hidden by steganography.
other's countries. We are increasingly dependent on mutual cooperation from other countries in investigating and prosecuting computer crimes....

To succeed in identifying and tracing global communications, we must work across borders, not only with our counterparts throughout the world, but also with industry, to preserve critical evidence such as log files, e-mail records, and other files, and we must be able to do so quickly, before such information is altered or deleted. If we cannot get this information quickly, the investigation may grow cold.8

Since cyber crimes take place at lightning speed, law enforcement organizations that are involved must be able to quickly establish collaborative partnerships with their peers wherever in the world they are located so they can work together in the rapid investigation of the crime and apprehension of the cyber criminal. As the trail can grow cold very quickly, law enforcement organizations need to be able to interact with their peers in other countries along two parallel tracks: (1) a fast track for ensuring that all available evidence of the cybercrime is quickly preserved and properly archived on a near real-time basis, and (2) a parallel, more deliberate track that works out complex legal details, such as proper jurisdiction.

At present, a framework for this level of collaboration does not exist in a consistent manner on a worldwide basis. However, an international policy consensus on the importance of meeting the threat of cybercrime has evolved, and initial encouraging steps have been taken.

B. CHALLENGES IN MAKING IT HAPPEN

1. The State of Affairs

(ii) Vulnerable Computers and Networks
In the rush to benefit from the Internet, many organizations often overlook engineering practices and technology that enhance security. Likewise, the pace of innovation presses on software developers, while the introduction of new products inevitably introduces new security vulnerabilities. At the same time, security holes continue to be found in

---

previous releases of computing and communications products that may still be in widespread use.

Typically, when these vulnerabilities are discovered, the vendor will quickly assess the nature of the problem and issue a patch that corrects the security flaw. The availability of the patch is announced via mailing lists and on websites with the intent that all system administrators using the product will quickly install the patch to correct that particular security vulnerability. In practice, this occurs unevenly and at any given time it is likely that the patch was not installed on many computers and networks, leaving them vulnerable to a problem the vendor patched several months, or even years, before. Moreover, it is not uncommon for the patch itself to have bugs, thereby creating new problems while trying to fix an old one.

In the end, the presence of a large number of vulnerable computers and networks provides many options to the cyber criminal.

(ii) Attack Tools Widely Available and Easy to Use
Significantly, all that the cyber criminal needs in order to engage in cybercrime is a personal computer and modem connected to the Internet; there are no significant equipment-related “barriers to entry” for engaging in cybercrime. Today’s intruder can choose from a menu of easily obtainable, increasingly sophisticated and automated attack tools. By using an automated scanner, cyber criminals can quickly and easily discover vulnerable computers that are connected to the Internet. Then they need only look at the specific nature of the vulnerability and select a script to exploit it in order to break into the computer. Once the break-in has occurred, a cyber criminal can use the compromised computer as a tool for committing the cybercrime of his or her choice. All of the above can happen at astonishing speed, and does not necessarily involve detailed knowledge regarding the internal working mechanisms of the automated scanners, exploit tools, and scripts used. To complicate matters further, tracks of the crime and the identity of the criminal often can be effectively masked through the use of anonymity tools.

(iii) The Virtual Nature of the Crime
Reconstructing a cybercrime can be extremely difficult, painstakingly slow, and sometimes impossible. It requires highly skilled technical personnel who are experts in the fields of networking and ICT forensics. Unlike investigations of traditional crimes, it is often impossible to contain the evidence by cordoning off the crime scene. For example, the evidence can be resident in a large number of computers located in many countries around the world. Many computers connected to the Internet are operated so that no logs
whatever are kept of the transactions and traffic that flows through them. Therefore, critical portions of evidence may simply not exist. Even when evidence does exist, it may be impossible to obtain because of legal issues. When evidence is obtained, analysis is highly complex and time consuming. Law enforcement personnel investigating cybercrime need to have available to them highly skilled technical personnel who are experts in the search and seizure of electronic evidence and in the field of forensics.

(iv) A Lack of Adequate Resources
Because of the nature of cybercrime investigations, there is a growing consensus among nations of the need to build cooperative, international processes for the investigation of cyber crimes. This will require all countries to make significant investments in staffing, training, and equipping their existing law enforcement organizations so that they are prepared to effectively collaborate with their peers on cybercrime investigations within a global network of law enforcement organizations.

Given the resources required, these investments will be most effective if made on a global, concerted basis. Industrialized countries are finding it difficult to ramp up to meet the challenges of cybercrime in a timely and cost-effective manner, and developing countries are at a loss of where and how to begin. They already face budget shortfalls and rely on donor organization assistance. The challenge of trying to introduce ICTs into a developing economy with inadequate infrastructure generally swallows available resources. Therefore, combating cybercrime is generally not a national priority. Cybercrime, however, cannot be effectively addressed if some countries connected to the Internet do not participate in global law enforcement initiatives. Countries that are unable to effectively address cybercrime will quickly become known as safe havens, and cyber criminals will use them as launching pads for their attacks or repositories for data on their cyber criminal activities.

(v) Competing Policing Priorities
Law enforcement’s battle against cybercrime is complicated by conflicting demands on existing resources. Most municipal and even national law enforcement organizations are sensitive to the needs of the public they serve. Police in large cities across the United States and around the industrialized world receive thousands of calls each day for a variety of criminal activities: robberies, rapes, homicides, drug trafficking, and gang activity are just some of the more common offenses reported. These crimes are immediately visible to the public eye; people can see drug dealers on the street corners, they know when
gangs gather in their neighborhoods, and homeowners instantly realize their ransacked home has been burglarized. It is, therefore, only logical that police would allocate extensive resources based on community demand and address violent crime and neighborhood disorder issues that are highly visible and frequently reported.

Unfortunately, computer crime is often invisible in nature. Frequently, individuals or organizations do not even know when they have been victimized. Given the relatively few people reporting hacking incidents to authorities, one can see why police chiefs dedicate fewer resources to cybercrime and it is given a lower priority. Of course, a lack of crime reports should not be taken to mean a lack of crime. Law enforcement must develop more sophisticated tracking mechanisms to better understand the true rates of cyber criminality and how it factors into traditional crimes. In addition, public outreach and education programs will help both businesses and individuals understand the serious threat posed by high-technology crime.

(vi) Inadequate Global Legal Environment
In order to deal effectively with cybercrime, it is not enough to simply invest in additional resources for law enforcement. It is very important that cybercrime laws around the globe be harmonized. Unless the differences and gaps in legal approaches can be rectified, the investigation and prosecution of cyber crimes will continue to be bogged down in a thicket of widely differing legal environments. It does little good if some countries update their laws to seriously address cybercrime if others are satisfied with weak laws, or worse yet, choose not to enact any laws at all.

Disparities in the international legal environment greatly handicap law enforcement activities and often make it impossible to proceed in investigating cybercrime cases and bringing the perpetrators to justice. The speed and flexibility of cybercrime attack scenarios (they can take place in an instant, or can be spread out over extended periods of time in a “low-and-slow” attack scenario that can be very difficult to detect) pose significant legal challenges to our traditional law enforcement environment. Particularly vexing legal issues include, but are not limited to, intercepting communications, searching and seizing electronic evidence, differing requirements for archiving logs of transactions and traffic generated at computer and communication systems, obtaining information from communication providers, and ensuring validity of cybercrime evidence across a variety of legal jurisdictions.

Private industry cooperation in sharing information with law enforcement agencies is also impacted by a variety of legal issues, such as antitrust, liability, privacy concerns, and fear of disclosure of shared
information through freedom-of-information laws that allow public access to government records. A successful legal regime must strike a balance between public safety and the freedom and privacy of industry and individuals.

(vii) Effective Leadership
Meaningful, coordinated changes to traditional law enforcement organizations are an extremely complex task that requires strong leadership capabilities and close public/private sector interaction. In the United States, for example, the vast majority of information technology products and networks are developed, owned, and operated by the private sector. Vendors must make it a priority to build security into their new products, while industry and citizens must urge government to provide law enforcement the tools, human resources, and laws to fight cybercrime. Rules and procedures for information sharing on threats and vulnerabilities need to be worked out so that a trust relationship can develop between government, industry, and citizens. On an individual level, people must be educated on the importance of being good cyber citizens.

2. On a National Level
The first steps toward effectively combating cybercrime can be taken at the national level. Although technology has dramatically advanced over the past few years, the practical needs of law enforcement in dealing with electronic crime have remained somewhat static. In 1998, the U.S. National Institute of Justice (NIJ) conducted a year-long study to identify the greatest shortcomings in U.S. law enforcement’s ability to address electronic crime. A total of 126 individuals from 114 agencies representing state and local law enforcement, bureaus of investigation, crime laboratories, transit police, and regulatory agencies participated in this exercise. By providing frontline perspectives to the challenges they were facing, the group was able to identify two overarching issues and ten top priority areas of need that are equally valid today. The overarching issues are:

- **Time Sensitivity.** All participants agreed that there was a grave risk that the ability to keep pace with cyber criminals would be exceeded by the capabilities of criminals and advancements in technology. Existing resources must be spent wisely and quickly, lest the criminals gain the upper hand.
- **Need to Maximize Investments.** A centralized, coordinated approach is needed when allocating resources to technical tools, training, onsite assistance, and research. The participants believed the
greatest impact would be achieved “if delivered through existing structures that have a broad reach and include most key stakeholders.”

The ten critical priority needs identified are:

1. **Public Awareness.** Information programs are needed to raise public awareness and educate citizens, elected and appointed officials, the criminal justice community, and industry on the incidence and impact of cybercrime. Although the CSI/FBI Computer Crime and Security Surveys from 1996 to 2002 note that the private sector’s willingness to report cybercrime to law enforcement has been on the rise, the fact remains that only 34 percent of the 2002 respondents reported intrusions to law enforcement.

2. **Data and Reporting.** Better data need to be collected regarding computer crimes and more sophisticated analysis performed and reported in order to better track and understand crime victimization and trends, budget appropriately, and realize the extent to which computers are being used in traditional crimes.

3. **Uniform Training and Certification Courses.** Entry-level and advanced training and certification programs based on predetermined national skill levels are needed to enable the proper investigation of crimes, the collection and examination of evidence, and the ability to appropriately handle cyber evidentiary issues in the courtroom. The intended audience includes police officers and investigators, forensic scientists, prosecutors, defense lawyers, probation and parole officers, and judges. Refresher and update courses also need to be offered to keep current with trends and technology.

4. **Cybercrime Task Forces.** Electronic crime task forces with regional or national capabilities for cyber investigations, forensic analysis, and public/private sector programs with industry are needed to bring efficiencies to the investigatory

---


10 NIJ Report at 3.

and evidentiary processes associated with electronic crimes. Specially trained personnel and dedicated forensic equipment are often required for the search and seizure and examination of electronic evidence. Not only have these task forces proven to enhance the process of investigating cyber crimes and make more efficient utilization of resources, they have also proven to be effective tools in combating cybercrime.

5. **Up-to-Date, Uniform Laws and Regulations.** There are wide discrepancies in laws and regulations concerning cybercrime on the state, federal, and international levels. A harmonized legal framework that is current with technological developments and use of technology would greatly facilitate investigations (such as consistency in the enforcement of subpoenas and criminal procedures).

6. **Cooperation with the High-Tech Industry.** It is important for law enforcement to maintain close cooperation with the high-tech industry. Areas where the high-tech industry can be most helpful to law enforcement include sponsoring training, participating in task forces, sharing equipment, raising public awareness, and encouraging the reporting of security breaches.

7. **Special Research and Publications.** A clearinghouse or resource point is needed for training materials, cybercrime information and research, technical guidance, information on new and specialized technologies, and lists of available security professionals.

8. **Management Awareness and Support.** It is important that senior-level law enforcement managers and elected officials understand the trends in cybercrime and the need for dedicated electronic crime units.

9. **Investigative and Forensic Tools.** Having up-to-date technological tools and equipment, including software, hardware (including data storage capacity), intrusion detection tools, and decryption technologies, is one of the most pressing, ongoing concerns of law enforcement and forensic scientists. The use of outdated technology can seriously hinder investigations and the ability to successfully apprehend and prosecute cyber criminals.

10. **Best Practices on Structuring Cybercrime Units.** Capturing and setting forth best practices in establishing electronic crime units (including organizational approaches) for the investigation and analysis of evidence would be especially helpful to law enforcement agencies with limited experience in this area.\(^\text{12}\)

\(^\text{12}\)NIJ Report at 3–6.
The U.S. government enacted its first computer crime laws in the mid-1980s. In the following decades, as the Internet revolution spread, the United States began to consider how best to meet the growing challenges of electronic crime. In the past few years, the U.S. government has been working in a variety of international fora to improve its ability to obtain electronic evidence and records from other countries. In addition, the U.S. public and private sectors have worked with the international community to improve information sharing capabilities and to create mechanisms that would facilitate the international exchange of electronic evidence and records. Overall, the U.S. government has taken several steps on a national level to address the priority issues set forth in the NIJ Report. U.S. actions continue to be consistent with its constitutional system of separation of powers and legal framework, including its commitment to freedom of information and protection of individual rights and privacy. Therefore certain aspects of its national efforts to combat cybercrime may not comport with differing legal systems.

(i) The Department of Justice

U.S. law enforcement has been at the forefront of worldwide efforts to fight the growing problem of cybercrime, and the Department of Justice (DOJ) has been a major contributor to that effort. The Computer Crime and Intellectual Property Section (CCIPS) is a special section of DOJ’s criminal division staffed with over two dozen specially trained lawyers who are experts in the legal, technological, and practical challenges of investigating and prosecuting cybercrime.13 The CCIPS serves as a central point of contact for investigators and prosecutors working on cybercrime cases. The unit provides legal advice and assists with court orders and arrangements pertaining to wiretaps and traps and traces on computer and communication networks. CCIPS lawyers have litigation responsibilities, are available on a 24/7 basis, and coordinate their activities with Assistant U.S. Attorneys, known as Computer and Telecommunications Coordinators (CTCs), who are stationed in field offices in each federal judicial district in the country and serve as each district’s expert on cybercrime.14 In addition, DOJ

---

13For a full array of information on DOJ’s Computer Crime and Intellectual Property Section, see http://www.cybercrime.gov.

14The CTC contact list can be found on CCIPS’s website at http://www.cybercrime.gov/CTClist.htm.
has worked with the National Association of Attorneys General to create a 50-state list of state and local computer crime specialists that is posted on the Internet.\textsuperscript{15}

On the international front, the CCIPS chairs the G-8 Subgroup on High-Tech Crime, which maintains a 24/7 Point-of-Contact Network for about 30 participating countries to help coordinate efforts in the investigation and prosecution of cybercrime cases. In addition, the CCIPS plays a leadership role in both the Council of Europe’s Experts Committee on Cybercrime and the Organization of American States’ cybercrime project.

In July 2001, U.S. Attorney General John Ashcroft announced DOJ’s creation of ten new, highly specialized \textit{Computer Hacking and Intellectual Property (CHIP)} units that would be dedicated to fighting cybercrime. The CHIP units are located in Alexandria, Atlanta, Boston, Dallas, Los Angeles, New York (Brooklyn and Manhattan), San Diego, San Francisco, and Seattle. Lawyers in the new CHIP units are responsible for prosecuting a wide range of computer crimes including computer intrusions or “hacking,” copyright and trademark violations, theft of trade secrets and economic espionage, theft of computer and high-tech components, fraud, and other cyber crimes. The new CHIP units further strengthen DOJ’s network of highly trained cybercrime prosecutors in the CCIPS and in the U.S. Attorneys’ offices. The CHIP teams work closely with industry to stay ahead of emerging cybercrime trends, identify new vulnerabilities in computer and communication systems, and prevent cybercrime from occurring at all.\textsuperscript{16}

The \textit{National Cybercrime Training Partnership (NCTP)} was established by DOJ to provide guidance and assistance to local, state, and federal law enforcement agencies in an effort to ensure that the law enforcement community is properly trained to address electronic and high-technology crime. The NCTP aims to develop a 21st-century model for law enforcement training in electronic and high-tech crime. NCTP training is up-to-date and is available to law enforcement investigators, forensic specialists, and prosecutors. The Partnership’s decentralized design enables it to reach law enforcement personnel in numerous geographic regions and levels of government. The NCTP


works in partnership with local, state, federal, and international law enforcement agencies.\textsuperscript{17}

The National Advocacy Center (NAC) is operated by DOJ’s Executive Office for U.S. Attorneys. The facility was built to train federal, state, and local prosecutors and litigators in advocacy skills and management of legal operations. The NAC expects to train more than 10,000 personnel annually.\textsuperscript{18} Programs for federal government personnel are provided by the Office of Legal Education of the Executive Office for U.S. Attorneys and by the National Bankruptcy Training Institute of the Executive Office for U.S. Trustees. Programs for state and local prosecutors are provided by the National District Attorneys Association (NDAA).\textsuperscript{19}

DOJ Criminal Division’s Fraud Section specializes in investigating and prosecuting cases of online fraud. The specific expertise of this Section is leveraged nationally and internationally through such initiatives as: the Internet Fraud Brief Bank training courses at the National Advocacy Center, an informational public website;\textsuperscript{20} and the Internet Fraud Complaint Center—a joint project of the FBI and the National White Collar Crime Center.\textsuperscript{21} Responding to new and evolving cybercrime threats, the Fraud Section provides national coordination of governmental efforts against identity theft through the Identity Theft Subcommittee of the Attorney General’s Council on White Collar Crime.

The Federal Bureau of Investigation (FBI) is DOJ’s principal investigative arm. It has the authority and responsibility to investigate specific crimes that are assigned to it, and is authorized to provide other law enforcement agencies with cooperative services, such as fingerprint identification, laboratory examinations, and police training. The FBI operates 56 field offices, approximately 400 satellite offices known as resident agencies, four specialized field installations, and more than 40 foreign liaison posts. The foreign liaison offices, each of which is headed by a Legal Attaché or Legal Liaison Officer, work abroad with

\textsuperscript{17}See \url{http://www.nctp.org} for more information on the National Cybercrime Training Partnership.

\textsuperscript{18}The NAC facility cost US$26 million to build and contains state-of-the-art courtroom presentation and audio/visual equipment. There are lecture halls of 50, 75, and 190 seats, a 440-person conference room, 10 training courtrooms, a 150-seat dining hall and kitchen, and 264 guest rooms. See \url{http://www.usdoj.gov/usao/eousa/ole/nacfacts.html} for more information on the National Advocacy Center.

\textsuperscript{19}See \url{http://www.ndaa-apri.org/} for more information on the National District Attorneys Association.

\textsuperscript{20}See \url{http://www.internetfraud.usdoj.gov/} for more information on Internet fraud.

\textsuperscript{21}See \url{http://www1.ifccfbi.gov/index.asp} for more information on the Internet Fraud Complaint Center and the National White Collar Crime Center.
American and local authorities on criminal matters within FBI jurisdiction. Approximately 9,800 employees work at FBI headquarters in Washington, D.C., while nearly 18,000 are assigned to field installations. The FBI has approximately 11,400 Special Agents and over 16,400 other employees who perform professional, administrative, technical, clerical, craft, trade, or maintenance operations.

The FBI houses the multiagency National Infrastructure Protection Center (NIPC) in Washington, D.C. The mission of the NIPC is to provide a national focal point for gathering information on threats to infrastructures, including cyber-based systems. A key NIPC mission is to build a bridge of trust to facilitate the sharing of information between private industry and citizens regarding intrusions and protective measures. NIPC performs its work through a variety of information products. NIPC Watch maintains an around-the-clock presence in the FBI’s Strategic Information and Operations Center (SIOC), which disseminates three levels of warnings and provides advisories on significant threats. To ensure the best possible coordination, the NIPC is staffed not only by law enforcement officials, but also by other U.S. agencies. The NIPC also works with trusted foreign law enforcement partners to share relevant information.

The FBI’s computer crime squads, which are stationed in 16 major metropolitan areas throughout the country, also coordinate their information with the NIPC. A major initiative of the FBI is the InfraGard program. InfraGard is a partnership between DOJ, industry, academia, and state and local law enforcement agencies. It is dedicated to securing critical infrastructures throughout the country, and now exists at each of the 56 FBI field offices. Nationally, InfraGard has over 5,000 members.

The Department of Justice, through its lawyers and investigators, uses foreign assistance funds provided by the Department of State to conduct training on the investigation and prosecution of cybercrime for its foreign law enforcement counterparts. This is a relatively small program, with future growth dependent on available resources. Funds are directed through the Overseas Prosecutorial Development Assistance and Training unit (OPDAT) of DOJ.

The FBI Academy provides training and operational functions for the FBI. Included on the complex is a Forensic Science Research and Training Center.

---

22 The NIPC maintains a website at http://www.nipc.gov.
23 See http://www.infragard.net for more information on the InfraGard program.
24 See http://www.fbi.gov/hq/td/academy/academy.htm for further information on the FBI Academy.
Another division of the DOJ that will have a role to play in combating cybercrime will be the Drug Enforcement Administration (DEA). The 2001 report of the United Nations International Narcotics Control Board (INCB) advised that drug traffickers worldwide are taking advantage of encrypted e-mail and other Internet technology to sell their products, launder money, monitor government law enforcement and border control measures, and trade tips and techniques to evade detection and capture. In light of these developments, the DEA is working to upgrade its ICT investigative capabilities.

(ii) The Department of State
The State Department has overall responsibility for the development and coordination of U.S. foreign policy. As such, the State Department elaborates the U.S. government positions in areas of cybercrime and cyber security in institutions like the G-8, the UN, the OAS, and other international fora. The State Department closely coordinates its activities with DOJ and other relevant U.S. agencies, including the private sector. The Office of the Legal Advisor, for example, worked closely with DOJ in the negotiations on the Council of Europe Convention on Cybercrime.

The State Department, through its International Narcotics and Law Enforcement Affairs (INL) Bureau, funds international law enforcement training and technical assistance. This includes courses in fighting cybercrime taught to foreign counterparts by DOJ/FBI, U.S. Customs, and U.S. Secret Service agents.

(iii) The U.S. Secret Service
The U.S. Secret Service in particular has been very active in combating cybercrime. In addition to its well-known protective responsibilities, the Secret Service has been investigating crimes since the mid-1800s. It has had primary responsibility for protecting U.S. currency and continues to work extensively with the financial services industry. Later, the Secret Service expanded its role to investigate crimes and fraud in the telecommunications industry. As the use of mobile telephones and third-party long-distance companies exploded, theft of service, cloning of cell phones, and manipulation of telecommunications systems became commonplace. The Secret Service has primary jurisdiction at the federal level for investigating these offenses.

The Secret Service built upon that experience to become heavily involved in combating cybercrime in the early 1990s. It developed its

---

26See http://www.ectaskforce.org/About_Us.htm.
Electronic Crime Special Agent Program (ECSAP), comprised of Secret Service agents—the same men and women who have substantial experience with both protecting the United States’ highest elected leaders and conducting criminal investigations. ECSAP agents also receive highly specialized training in the forensic analysis and preservation of electronic evidence. They are computer investigative specialists, qualified to conduct investigations in all types of electronic evidence, including computers, networks, telecommunications devices, smart cards, and electronic organizers. To date, the Secret Service has trained 175 ECSAP agents and placed at least one in all Secret Service field offices across the country.

Beyond its successful ECSAP program, the Secret Service has developed what many believe to be a model for law enforcement in the information age. In 1995, the Secret Service formed a nationwide electronic crimes task force based in its New York field office. Since its inception in 1995, the New York Electronic Crimes Task Force (NYECTF) has charged more than 800 individuals with electronic crimes valued at more than US$425 million. It has recovered more than 2,000 cloned cell phones, and resolved approximately 2,100 identity thefts. Perhaps most important, the task force has trained more than 11,000 law enforcement personnel, prosecutors, and private industry representatives in the criminal abuses of technology and how to prevent them. The NYECTF stresses a cooperative model of enforcement between the private sector and government, and, thus, is fairly unique in its approach to combating high-tech crime. The U.S. Congress recently recognized the value of the NYECTF when it included its work in the USA PATRIOT Act and rolled out similar electronic crime task forces nationwide. Congress also expanded the role of the Secret Service in combating high-tech crime.

(iv) The U.S. Customs Service
The U.S. Customs Service (USCS) manages a CyberSmuggling Center and provides training to U.S. and foreign law enforcement on combating ICT crime. It is heavily involved with the Smart Borders initiatives with Canada and Mexico and international efforts to provide greater security for maritime container traffic. Such initiatives will require developing enhanced law enforcement capacity to detect and prevent cybercrime.

28See http://www.customs.ustreas.gov/enforcem/cyber.htm for more information on the Customs CyberSmuggling Center.
(v) The Federal Law Enforcement Training Center

The Federal Law Enforcement Training Center (FLETC) is a partnership of federal law enforcement organizations. Its mission is to provide quality, cost-effective training for law enforcement professionals. This mission is accomplished by (a) utilizing law enforcement and training experts; (b) providing quality facilities, support services, and technical assistance; (c) conducting law enforcement research and development; and (d) sharing law enforcement technology.29

(vi) Homeland Security Considerations

In June 2002, the Bush Administration proposed the creation of a new Department of Homeland Security, a cabinet-level agency that would have as its primary mission the prevention of terrorist attacks within the United States, the reduction of the U.S.’s vulnerability to terrorism, and the minimization of any damage, and assistance in the recovery, from any attacks that may occur.30 Among the many existing federal agencies and functions proposed for inclusion in this new department are several law enforcement agencies with missions that include promoting cyber security and fighting cybercrime.

As originally drafted, The Homeland Security Act of 2002 (HS Act)31 would create four new undersecretary positions, one of which, under Title II—Information Analysis and Infrastructure Protection (IAIP), would (a) oversee law enforcement information and intelligence, (b) assess vulnerabilities of key infrastructures, (c) identify protective priorities and take steps to protect them, (d) develop a national plan, (e) administer a Homeland Security Advisory System, and (f) review and make recommendations for improvement in information sharing among federal agencies and between the federal and state and local governments. The following agencies with cybercrime and cyber security related functions would be transferred to IAIP: the National Infrastructure Protection Center (NIPC) of the FBI, the Critical Infrastructure Assurance Office (CIAO) of the Department of Commerce, the Computer Security Division of the National Institute of Standards and Technology (NIST), the National Infrastructure Simulation and Analysis Center of the Department of Energy, and the Federal Computer Incident Response Center of the General Services Administration.

---


31 The full text of the Homeland Security Act of 2002 can be found at http://www.whitehouse.gov/deptofhomeland/bill/index.html. At press time of this publication the act is under active review and revision.
Of particular interest is Section 204 of the HS Act, which deals with “sharing of information with the Department of Homeland Security by the private sector, state and local governments, and individuals.” As currently written, the HS Act would provide a FOIA exemption for information voluntarily provided that relates to infrastructure vulnerabilities and other vulnerabilities to terrorism. If implemented, this protection could have a significant impact on the willingness of private industry to report computer intrusions—potentially leading to more federal prosecutions of cybercrime.

Other existing federal agencies with a cybercrime role affected by the new legislation include the U.S. Customs Service, which, under Title IV of the HS Act, will be overseen by an Undersecretary for Border and Transportation Security. The inclusion of Customs would add its Cybersmuggling Center to the new agency. How the center, with a significant overseas agenda in fighting transnational ICT related crime, will adapt to joining an agency focused on domestic security and terrorism remains to be seen. Similarly, the U.S. Secret Service, which would be transferred under Section 720 of the HS Act as a “distinct entity” within the new department, has a cybercrime capability in its areas of competence and an international agenda that would need to be adapted to the new department.

Overall, the evolution of the new department will be of particular interest to those who support a strong public/private partnership in fighting cybercrime. The NIPC is presently an integral part of the existing U.S. government scheme for fighting cybercrime, working with the FBI as the lead federal law enforcement agency managing outreach to the private sector (through its InfraGard program). Although the Computer Investigations and Operations Section will remain, the transition of the rest of the NIPC to the new department would need to be carefully managed to avoid confusion, loss of private sector trust, and loss of effectiveness. Similarly, the CIAO is the lead federal agency building partnerships with civilian ICT industry on cybersecurity. The inclusion of CIAO in an organization structured to fight terrorism in close cooperation with U.S. law enforcement, defense, and intelligence agencies could cause tension with the private sector over privacy and liability issues. Unless a balance is struck between government and industry on these issues, the resulting friction could set back efforts to build the necessary public/private partnerships—partnerships that must be voluntary to fully succeed.

Finally, all of the federal law enforcement agencies proposed for transfer to the Department of Homeland Security have significant international components to their mission statements. These will have to be reconciled in their new environment as part of a department focused on the defense of the geographic United States.
Overall, the United States is working very hard to foster effective law enforcement cooperation worldwide. At the national level, a number of government departments such as the Departments of State, Justice, Treasury, and Commerce are already deeply involved with international initiatives that specifically target cybercrime. These initiatives have spread across a wide range of multilateral fora such as the United Nations (UN), the Group of Eight (G-8), the Council of Europe (CoE), the European Union (EU), the Organization for Economic Cooperation and Development (OECD), the Asia-Pacific Economic Cooperation organization (APEC), and the Organization of American States (OAS).

(vii) Legal Considerations

Variations among U.S. domestic laws and the laws and legal institutions of foreign countries are a significant barrier to obtaining and receiving international legal cooperation. To the extent that differences in the laws of various countries pose an impediment to foreign law enforcement assistance, DOJ has concentrated on international outreach efforts as a remedy.

Mutual Legal Assistance Treaties (MLATs) are one important tool. MLATs seek to improve the effectiveness of judicial assistance and to standardize its procedures. Under an MLAT, each country designates a central governmental authority that communicates directly with other nations’ central authorities concerning requests for international assistance in criminal investigations. Generally, the Justice Department serves as the U.S. central authority, while Ministries of Justice fulfill the equivalent role in foreign nations. MLATs permit the central authority to summon witnesses, to compel the production of documents and other real evidence, to issue search warrants, and to serve process. Generally, the remedies offered by the treaties are available only to prosecutors.

The MLAT process has frequently been used to obtain and provide digital evidence in international computer crime investigations. The United States is frequently asked, through the G-8 24/7 Point of Contact Network, to assist in obtaining information related to computer attacks and intrusions that emanate from servers located within U.S. borders. Upon receipt of such a request, DOJ may request, pursuant to 18 U.S.C. Section 2703(f), that the communications service provider preserve the information. Thereafter, the requesting country’s central authority

32The text of this provision can be found at http://www4.law.cornell.edu/uscode/18/2703.html.
of its Ministry of Justice will work with DOJ to obtain the requested information. The process works the same when the United States requests assistance from other countries. However, some of the countries from which data is requested do not have data preservation authority, which may result in loss of the information needed for an investigation. Moreover, if national laws direct providers to immediately destroy personal identifying information not necessary for billing or other limited purposes upon termination of a communication, the data are irretrievably lost. This has been a major point of contention between the United States and the European Union, as the directive concerning the processing of personal data and the protection of privacy in the telecommunications sector mandates the destruction of such data.33

Handling incidents wherein no MLAT or other extradition treaties exist can be extremely frustrating for law enforcement. In those instances, informal law enforcement connections can provide a useful source of assistance. For example, were there no MLAT or other treaty between the United States and Tanzania, and an FBI agent needed something from the Tanzanian government, the agent might contact the U.S. Embassy in Dar es Salaam and speak to the legal attaché there. The legal attaché, in turn, could try to ask a local police official to provide assistance. While these informal networks can be highly effective, their lack of formalization can also be problematic. While a police officer in Dar es Salaam might be willing to obtain computer logs from the local ISP on behalf of the FBI as a favor, there would be little he might be able to do vis-à-vis formal extradition proceedings. The other problem with informal networks is that the average police officer in one country frequently does not have many contacts in the other country. Thus, the system of informal assistance is quite spotty

and depends on the ability of the local investigator or prosecutor to network well beyond his or her traditional circle of professional contacts.

The *Federal Rules of Criminal Procedure* can limit the U.S. government’s ability to share requested information with other countries. For example, Federal Rule of Criminal Procedure 6(e) imposes limits on the disclosure of information concerning matters before a federal grand jury. Information collected by the grand jury may be disclosed only for limited purposes enumerated under Rule 6(e). There is no provision under Rule 6(e) that expressly permits disclosure of grand jury information to a foreign country. It is possible, however, that such disclosure could be made under Rule 6(e)(3)(C)(i)(I), which provides:

> Disclosure otherwise prohibited by this rule of matters occurring before the grand jury may also be made—
> 1. when so directed by a court preliminary to or in connection with a judicial proceeding.

Rule 6(e) information that is shared with a foreign country pursuant to a court order is likely to be subject to restricted handling procedures.

Similarly, limitations on dissemination may also occur for information obtained under other provisions of federal criminal law. For example, Title III of the *Omnibus Crime Control and Safe Streets Act* (Title III), which provides authority for conducting wiretaps, limits disclosure of the contents of the intercepted communications. Again, while Title III does not expressly permit disclosure of wiretap information to foreign countries, under appropriate circumstances pursuant to 18 U.S.C. Section 2517(5),\(^{34}\) it is possible to obtain authorization for disclosure from a federal court.

The *Federal Rules of Evidence* also raise important admissibility and evidentiary issues when computer records are presented in court. Critical issues concern (a) the authentication of the record (that it is what it is claimed to be), (b) the integrity of the record (that it has not been altered), (c) the reliability of the computer-generated records (the program that generated them did not contain serious programming errors and could be relied upon), and (d) the identity of the author (authenticating the author of the computer-generated records). The Federal Rules of Evidence also bar evidence deemed to be hearsay (out-of-court statements/assertions by persons that are deemed part of

---

\(^{34}\)The text of this provision can be found at [http://www4.law.cornell.edu/uscode/18/2517.html](http://www4.law.cornell.edu/uscode/18/2517.html).
the digital evidence). Usually, computer-generated records are admissible under the business records exception to the hearsay rule, unless they contain human statements. The Best Evidence Rule requires a writing, recording, or photograph to be an “original.” Fortunately, the rule explicitly accepts digital data as an original.35

4. International Law Enforcement Cooperation Initiatives

International law enforcement initiatives can leverage national efforts and create momentum for change. The global developing legal framework regarding ICTs, including cybercrime, is being driven from the top down: Multinational organizations such as the EU, OECD, CoE, WTO, UN, and APEC are having a profound influence upon the legal and policy developments in nation states. Developing countries should actively participate in global discussions and ensure that their cybercrime initiatives are in step with global developments.

(i) Group of Eight (G-8)

The G-8 country economies account for 48 percent of the global economy, 80 percent of economic activity in developed economies, and 49 percent of global trade.36 G-8 leaders meet in person every year to discuss key issues. Consistent with earlier actions, Article 33 of the Communique issued at the 2001 summit affirmed the G-8’s commitment to combat international organized crime. The G-8 strongly endorsed the outcome of the G-8 Justice and Interior Ministers’ Conference37 held in Milan, Italy, earlier that year, and it encouraged “further progress in the field of judicial cooperation and law enforcement, and in fighting corruption, cybercrime, online child pornography, as well as trafficking in human beings.”38

The U.S. government has been working with the G-8 to improve the channels for obtaining assistance in cybercrime matters. Participants in the G-8’s Subgroup on High-tech Crime have begun to develop a

comprehensive set of options for improving the ability to locate and identify criminals who use ICTs to conduct or facilitate crimes. Within the G-8, a 24/7 Point of Contact Network of law enforcement has been established and is already operational. Its main purpose is to receive and respond to urgent requests for cooperation in cases involving electronic evidence. The network has been used successfully in a number of cases. These contact points supplement existing structures of mutual assistance and channels for communications. Currently, over 30 countries are participating in the 24/7 Point of Contact Network.

Another important G-8 effort was the 1998 adoption of ten Principles to Combat High-Tech Crime. These principles later became the basis for policy recommendations within the UN and the Organization of American States.

(ii) Council of Europe (CoE)
The Council of Europe (CoE) consists of 44 Member States, including all of the members of the European Union. The CoE was established in 1949 primarily as a forum for upholding and strengthening human rights and promoting democracy in Europe. Over the years, the CoE has been the negotiating forum for a number of Conventions on criminal matters in which the United States has participated. For the last few years, the CoE has been working on the Convention on Cybercrime (CoE Convention).

The CoE Convention breaks new ground by being the first multilateral agreement drafted specifically to address the problems posed by the international nature of computer crime. The CoE Convention requires signatory countries to establish certain substantive offenses in the area of computer crime and requires parties to adopt domestic procedural laws to investigate computer crimes. It also provides a solid basis for international law enforcement cooperation in combating crime committed through computer systems. The CoE Convention was opened for signature on November 23, 2001. To date, it has been signed by 29 of the 44 CoE Member States and four partner countries: U.S., Canada, Japan, and South Africa. The U.S. House of Representatives has signed the CoE Convention and is expected to forward it to the U.S. Senate for advice and consent during its 2002 session.

(iii) European Union (EU)

The European Union represents 15 nations and more than 370 million people. An additional 13 eastern and southern European nations are in the process of joining the union. The EU has a growing number of initiatives aimed at fighting high-tech and transnational crime.

At the outset, it is important to note that the EU has addressed the issue of cybercrime at its highest substantive policy levels. On January 6, 2001, the European Commission (the executive body for the EU) issued a communication addressed to the Council, the European Parliament, the Economic and Social Committee, and the Committee of the Regions entitled “Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime.” This document is commonly referred to as the “EC Cybercrime Communication” and addressed such topics as threats, substantive and procedural law issues (such as interception of communications, retention of traffic data, anonymous access and use, and practical cooperation at the international level), and jurisdictional issues. It proposed both legislative and non-legislative measures.

The EU has also addressed cybercrime through the European Police Office (Europol). Headquartered in The Hague, The Netherlands, Europol is the EU’s law enforcement organization responsible for improving the effectiveness and cooperation between competent authorities in EU Member States. It was established on February 7, 1992, under the Treaty on European Union and is accountable to the Council of Ministers for Justice and Home Affairs. Europol became fully operational on July 1, 1999. Its mandate includes preventing and combating terrorism, drug trafficking, and other serious forms of international organized crime, such as immigration networks, vehicle trafficking, trafficking in human beings including child pornography, forgery of money and other means of payment, money laundering, and trafficking in radioactive and nuclear substances.

Europol has approximately 250 members on staff, all of whom have been assigned by various EU member nations. Approximately 45 of these staff members—known as Europol Liaison Officers (ELOs)—represent their nations’ various law enforcement agencies such as

---

police, customs, gendarmerie, and immigration services. Europol recently completed the phased deployment of The Europol Computer System (TECS). The new computer system is specifically designed to facilitate the sharing and analysis of criminal data between EU member nations and law enforcement organizations in other countries. Each EU member nation has assigned two Data Protection Experts to Europol to closely monitor how personal data are stored and used.

In September 2000, the EU’s Council of Ministers for Justice and Home Affairs asked EU member nations to start responding to requests from Europol to investigate specific cases and keep Europol informed about the status and results of the investigation. Since November 2000, EU member nations have been able to leverage the resources of Europol National Units (ENUs) on joint investigations in accordance with the Europol Convention and its implementing rules. The European Police Chiefs Operational Task Force coordinates its activities with Europol in combating transnational crime.

The Maastricht Treaty (1993) made judicial cooperation in criminal matters a high priority for EU Member States. Subsequently, the European Council adopted an Action Plan (1997) to improve the level of cooperation between the judicial authorities of EU Member States. This resulted in the launch in 1998 of the European Judicial Network (EJN), which is a “decentralised network between EU lawyers and judges working on criminal cases and tries to help them exchange information rapidly and effectively.” The EJN maintains specialist contact points in all EU Member States. The Amsterdam Treaty (1999) further reinforced the importance of efficient and effective transnational judicial cooperation.

Work is under way within the EU on establishing Eurojust, a new centralized service that was proposed in October 1999, by a special meeting of the European Council in Tampere, Finland. Eurojust is

---

44See http://www.europol.eu.int/content.htm?links/en.htm for links to EU Member States’ national law enforcement websites, links to European institutions and international organizations, and links to other law enforcement agencies and organizations.
45The text of the Europol Convention can be found at http://www.europol.eu.int/content.htm?legal/conv/en.htm.
48See http://ue.eu.int/ejn/ for more information on the European Judicial Network.
intended to facilitate cooperation at the judicial level between the legal systems of various EU Member States. The centralized design of the Eurojust service is intended to complement the inherently decentralized nature of the EJN. Resources available through Eurojust will include senior lawyers, magistrates, prosecutors, judges, and other legal experts representing every EU member state. The intent is to greatly speed up the collaborative process by having all necessary legal resources in the same location, working together as a close-knit team. While Eurojust will be able to make legal recommendations to the relevant authorities in each of the EU Member States, it will not have the necessary authority to directly and independently undertake such investigations itself.\(^{51}\)

The European Anti-Fraud Office (OLAF) was established in 1999 as the successor organization to the Task Force for the Coordination of Fraud Prevention. It was established as an independent organization responsible for investigating fraud, corruption, and any other illegal activity that could potentially impact EU financial interests. The approximately 280 agents who work for OLAF are highly experienced in investigating complex fraud cases. OLAF reaches out to all European citizens for information on fraud by maintaining toll-free hotlines accessible from every EU member state.\(^{52}\)

The eEurope Action Plan\(^{53}\) of 2000 and the more recent eEurope 2005\(^ {54}\) Action Plan address security concerns related to increasing global cybercrime. The various directives and safeguards for e-commerce are intended to establish an improved legal framework for e-commerce as well as protect the EU’s communication networks and ICT infrastructure. They augment several initiatives that are already under way within the EU to combat harmful and illegal content on the Internet and protect intellectual property rights and the confidentiality of personal data.


\(^{52}\)See http://europa.eu.int/comm/dgs/olaf/ for more information on the European Anti-Fraud Office.


(iv) International Criminal Police Organization (Interpol)

Founded in 1923 and located in Lyon, France, since 1989, Interpol is an important link among law enforcement organizations globally.\(^55\) Interpol has 178 member countries and maintains close working relationships with dozens of intergovernmental bodies such as the Council of Europe and World Customs Organization. Interpol’s primary mission is to promote the widest possible mutual assistance between all criminal police authorities.

Interpol has a system of offices around the world referred to as National Central Bureaus (NCBs). Each of its 178 member nations has an NCB station, generally within that nation’s capital. One or more local law enforcement agencies are responsible for staffing the NCB and will represent national law enforcement to Interpol. For example, in Canada, the Royal Canadian Mounted Police (RCMP) staff and support the NCB in Ottawa. Should a police officer in Montreal or Winnipeg need something from the police in Gaberone, Botswana, the Montreal police would route their request through their police computer systems to the NCB in Ottawa. The RCMP staff would then forward that request via a private encrypted computer network to the Interpol Secretariat General in Lyon, France. The bureau receiving the message at the Secretariat would read the message and forward it to the necessary agency in Botswana. Each of the 178 countries participating in the Interpol system has access to special computer and telephone systems to facilitate the transfer of this information.

Interpol has been actively involved in combating Information Technology Crime (ITC) for a number of years. The Interpol General Secretariat has harnessed the expertise of its members in the field of ITC through “working parties” or groups of experts. Each working party consists of the heads or experienced members of national computer crime units. They are designed to reflect regional expertise and are established in Europe, Asia, the Americas, and Africa, although each is in different stages of development. In addition, Interpol has created several handbooks and computer crime manuals that it distributes to law enforcement agencies worldwide to use as best practice guides. Interpol currently has a number of ongoing projects related to high-technology crime, including information sharing mechanisms for law enforcement and a 24-hour/7-day-a-week point-of-contact network to allow investigators in one jurisdiction to locate and communicate with their counterparts abroad.\(^56\)

\(^{55}\)See http://www.interpol.int/.

\(^{56}\)See http://www.interpol.int/ for further information on Interpol.
Organization for Economic Cooperation and Development (OECD)

The OECD, which maintains a permanent secretariat in Paris, France, is comprised of 30 member countries that share a commitment to democratic government and the market economy. It provides a global forum for discussions on difficult international issues, fostering better-informed work within member nations’ own governments, and helping to clarify the impact of national policies on the international community. The OECD is known for its “soft law,” that is, nonbinding instruments on a variety of difficult public policy issues that have global impact. For example, it is at the forefront of efforts to understand and help governments respond to new challenges such as sustainable development, electronic commerce, biotechnology, and food safety. Given the global nature of cybercrime, the OECD has an important role to play in fostering good governance in this area.

It is becoming increasingly clear that disparities in national policies on emerging e-commerce issues could result in obstacles to the development of global communication networks and hinder international trade. Recognizing this, the OECD is working with member nations and other governments on developing an internationally coordinated approach to facilitate the development of secure, global communication networks and ICT infrastructures. It is doing this by helping to rapidly generate consensus on difficult policy and regulatory issues such as those relating to cryptography, privacy, data protection, and the security of information systems.

For example, in 1996, the OECD Committee for Information, Computer and Communications Policy (ICCP) formed the Ad hoc Group of Experts on Cryptography Policy Guidelines to address emerging issues in cryptography policy. The Ad hoc Group quickly identified and examined issues of importance in the national and international debate on cryptography policies, and produced a set of guidelines that were adopted as a “Recommendation of the Council of the OECD” in 1997. To facilitate public discussion of the guidelines, the OECD published a document entitled OECD Cryptography Policy Guidelines and the Report on Background and Issues of Cryptography Policy, which explained the context for the Guidelines, discussed the basic issues involved in the international cryptography policy debate, explained the need for international action on cryptography policy, and summarized relevant work in the area by the OECD and other organizations.

The OECD Guidelines for the Security of Information Systems,58 adopted in 1992, are reviewed every five years. They were not changed in the 1997 review, but they were revised in 2002 by the OECD’s Working Party on Information Security and Privacy (WPISP) to take account of changes in the development of interconnected and interdependent information systems.59 These guidelines are relevant to cybercrime in that they address the need for business and government to develop mechanisms to share information regarding threats and defensive measures.

(vi) United Nations (UN)
The UN established its first office for fighting international crime in 1948. Today, the UN is very well positioned to play the role of an impartial organization with which all countries of the world can work in addressing increasingly important cross-border problems such as those posed by organized transnational crime.

At the policy level, the U.S. recently sponsored and obtained General Assembly approval for two resolutions related to high-tech crime. A/RES/55/63, “Combating the criminal misuse of information technologies,” adopted December 4, 2000, noted the value of the ten principles set forth by the G-8 Experts to combat criminal misuse of information technology. The ten principles are:

- States should ensure that their laws and practices eliminate safe havens for those who criminally misuse information technologies.
- Law enforcement cooperation in the investigation and prosecution of international cases of criminal misuse of information technologies should be coordinated among all concerned States.
- Information should be exchanged between States regarding the problems they face in combating the criminal misuse of information technologies.
- Law enforcement personnel should be trained and equipped to address the criminal misuse of information technologies.
- Legal systems should protect the confidentiality, integrity, and availability of data and computer systems from unauthorized impairment and ensure that criminal abuse is penalized.

Legal systems should permit the preservation of, and quick access to, electronic data pertaining to particular criminal investigations.

Mutual legal assistance regimes should ensure the timely investigation of the criminal misuse of information technologies and the timely gathering and exchange of evidence in such cases.

The general public should be made aware of the need to prevent and combat the criminal misuse of information technologies.

To the extent practicable, information technologies should be designed to help prevent and detect criminal misuse, trace criminals, and collect evidence.

The fight against the criminal misuse of information technologies requires the development of solutions taking into account both the protection of individual freedoms and privacy and the preservation of the capacity of Governments to fight such criminal misuse.60

A/RES/56/121, adopted December 19, 2001, again urged Member States to take these principles into account in developing their policies against cybercrime.61

The United States has taken a strong position in urging UN Member States to consider these principles in devising their own legal regimes. While some Member States have raised an interest in a global instrument against cybercrime, the United States has come out firmly against this idea, contending that such a instrument would be premature given the varied levels of legal and ICT development of UN Member States and the need to allow existing efforts, like the Council of Europe Cybercrime Convention, an opportunity to be observed in practice.

In the development of data for future action, the UN Centre for International Crime Prevention (CICP) works with individual UN Member States to orchestrate a coordinated global response to the growing problem of international crime. Based in Vienna, Austria, the CICP employs about 15 professional staff members (plus support personnel) and is a part of the UN Office for Drug Control and Crime Prevention. It cooperates with a network of international and regional institutions on issues in crime prevention, criminal justice, and criminal law reform. In

addition, the CICP takes a special interest in combating transnational organized crime, corruption, and illicit trafficking in human beings.\(^62\)

In the battle against international crime, the CICP plays an important role in helping establish a common global framework respectful of human rights and sensitive to the needs of individuals. The internationally recognized principles that it defines have been adopted by more than 100 countries in drafting their own national legislation and policies in matters of independence of the judiciary, protection of victims, alternatives to imprisonment, treatment of prisoners, police use of force, mutual legal assistance, and extradition.

In partnership with its Turin, Italy–based research arm, the UN Interregional Criminal Justice and Research Institute (UNICRI), the CICP researches and studies new and emerging forms of crime.\(^63\) It assists UN member nations in leveraging the latest information technology techniques in the collection, analysis, and utilization of criminal justice data. The CICP also maintains the Internet-based UN Crime and Justice Information Network (UNCJIN), which is a database of crime statistics, publications, and links to UN agencies and other research organizations and universities.\(^64\)

The CICP has proposed three global Programmes that address topical concerns of the international law enforcement and legal community but are related to cybercrime because of the increasing role ICTs are playing in these activities. These are: (1) the Global Programme against Corruption, (2) the Global Programme against the Trafficking in Human Beings, and (3) the Global Programme against Transnational Organized Crime.\(^65\)

Recognizing that organized crime had become too widespread for any single nation to address on its own, UN member nations joined forces to propose the UN Convention Against Transnational Organized Crime.\(^66\) The Convention establishes a common framework for harmonizing different legal systems that exist in each country and highlights the importance of a legally binding instrument to overcome problems traditionally encountered with international cooperation and mutual assistance.


\(^{63}\)See http://www.unicri.it/index.htm for further information on the UN Interregional Criminal Justice and Research Institute.

\(^{64}\)See http://www.undcp.org/uncjin.html for further information on the UN Crime and Justice Information Network.

\(^{65}\)See http://www.undcp.org/crime_cicp.html for further information on these Programmes.

\(^{66}\)For further information on the UN Convention against Transnational Organized Crime, see http://www.undcp.org/odccp/crime_cicp_Convention.html.
The 10th UN Congress on the Prevention of Crime and the Treatment of Offenders took place in Vienna, Austria, in April 2000, and, among other issues, highlighted new developments in crime prevention and crimes related to computer networks. A technical workshop held during the Congress addressed topics in computer crime.

(vii) Organization of American States (OAS)

Cybercrime has also arisen on the agenda of the OAS. In a March 1999 meeting of Ministers and Attorneys General of the Americas, the OAS recommended the establishment of an intergovernmental group of experts on cybercrime. The group had a mandate to survey the state of national legislation, policies, practices, and expertise related to cybercrime and to identify mechanisms of cooperation within the Inter-American system. The results of this survey were provided in October 1999 in a Final Report on the Meetings of Government Experts on Cyber Crime. The G-8 Principles have also been favorably received at the OAS. The Third Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas, which convened in San Jose, Costa Rica, on March 3, 2000, approved ten recommendations tracking the G-8 Principles. The Inter-American Committee on Terrorism (CICTE) included cyber terrorism in its declaration of principles at its January 2002 meeting.

(viii) Asia Pacific Economic Cooperation (APEC)

APEC has begun to consider computer crime and computer security issues within the ambit of member state efforts to develop a positive international environment for global e-commerce. At their October 21, 2001, meeting, APEC Economic Leaders adopted a statement on counter-terrorism that included strengthening APEC activities in

---


70 See http://www.oas.org/juridico/english/docu2.htm for information on the nature, powers, and functions of the CICTE.
III. Practical Considerations

A. THE REALITY: HOW TO RESPOND

The realities of combating cybercrime are harsh. The evidence can be resident on a large number of computers and communication systems located in multiple countries. Traditional international procedures, with their focus on local jurisdictional environments, are often starkly inadequate in the effective prosecution of cybercrime. Mechanisms for cooperation between the law enforcement organizations of the countries involved in any given case simply may not exist.

Even when there is a clear basis in law for international cooperation, technical problems could make it impossible. For example, the log file archives that contain critical transaction/traffic records may not exist or may not have been preserved. In addition, it may be impossible to contact and quickly mobilize appropriate technical, prosecutorial, and
judicial staff in key foreign countries. Cyber criminals could also use strong encryption or other technologies that defeat government capabilities.

Should a criminal be charged, inadequate laws and treaties can make it difficult to convict the person. There may be a tendency in some parts of the world for law enforcement to regard computer crime as an exotic and less harmful act not worthy of the full weight of prosecution. Penalties may be weak or nonexistent. In nations with a weak rule of law, cyber criminals can engage in criminal conduct confident that it is highly unlikely that they will ever have to face the consequences. The need for a well-defined and internationally accepted legal framework for dealing with cybercrime is urgent. Absent that, every country must be ready, willing, and able to quickly mobilize the necessary resources for joint cybercrime investigations when requested to do so by law enforcement organizations in other countries.

In the meantime, law enforcement must respond. Law enforcement officers in developing countries must understand how to respond to computer crime calls, especially when it is determined that the crime involves communications or activities beyond their sovereign borders. Some initial steps to take include:

- Clues of cybercrimes may be found in computer logs—if logs are kept—that a trained law enforcement officer can use to trace the route of communications from computer to computer, using the Internet Protocol address. If the log has not been modified by the hacker, it should indicate the exact address of the computer from which unauthorized access was made. Attacks are often launched through numerous “hops” between computers to disguise the identity of the attacker. Therefore, an investigator may have to track back through several computer hops to determine the origination point. The identity of the owner of the computers may be determined through the American Registry of Internet Numbers.  

- Subpoenas, court orders, and search warrants may need to be issued to communication providers and/or the attacker (if identified) for each hop.

---

74 See http://www.arin.net/tools/whois_help.html for information on conducting a WHOIS database search and other useful information.

75 In this context, “communication provider” is intended to include all types of communications, including ISPs, telephony, cable, wireless, and satellite companies.
If the law enforcement officer determines that the communication was routed outside the sovereign borders of his or her nation, the officer must go to the proper authority (usually the Ministry of Justice) to see how to proceed in making a request for the information. Usually, this means determining if the country from which information is needed (a) has an MLAT in place with the requesting country, (b) if it is a participant in the G-8 24/7 Point-of-Contact Network, (c) if the country will voluntarily cooperate, or (d) if the requesting country has a Letters Rogatory process that must be followed in order to obtain the information.

When making the request, terminology differences can determine whether the request is properly understood. It is important to clearly state what information is needed and, if possible, determine what terminology the country or communications provider in the country from which information is needed uses to identify the same information.

If the data have not been destroyed, the prosecutor from the requesting country should send a retention letter requiring the communications provider to preserve stored records, communications, and other evidence. The request will have to comply with any statutes governing this process.76

The requesting officer may need assistance identifying, locating, and interviewing witnesses. This may require transmitting detailed instructions setting forth the desired procedures that should be taken in gathering the evidence.

The law enforcement officer should seek the consent of the victim to obtain any evidence that may be helpful to the investigation. Contents of a hacker's communications that are stored on the victim's computer can be very helpful. If image copies are going to be made of this evidence, this must be performed by trained personnel such that the integrity of the data is preserved.

If live surveillance is desired, it usually will be necessary to obtain wiretap, pen register, or trap-and-trace court orders—possibly one for each communications provider, and perhaps even by jurisdiction of the provider. The law enforcement officer

---

76In the United States, such retention letters are governed by 18 U.S.C. Section 2703(f); the text of this provision can be found at http://www4.law.cornell.edu/uscode/18/2703.html. The action taken by the country from which information is requested will generally have to comport with the laws governing such searches and seizures, interviewing of witnesses, etc.
may also want to seek an order directing the communications provider not to disclose to the customer that the information has been requested.77

■ If the hacker has been identified, the law enforcement officer from the requesting country should seek a search warrant to obtain the hacker’s computer and other relevant materials. Again, detailed instructions to accompany the warrant may be required.78

■ If extradition is desired, the prosecutor will have to determine (a) whether an extradition treaty with the country where the hacker resides is in effect, (b) whether dual criminality or other exceptions will enable the country to refuse to extradite, and (c) what legal procedures must be followed.

Common Questions

Q: When does a country send its law enforcement officer to assist in the country from which information is being requested?

A: Generally speaking, law enforcement officers from one nation have absolutely no jurisdiction or authority in a foreign territory. This is often true within a nation as well. For example, a San Francisco police officer who witnesses a crime in Chicago has no more power to arrest than an average citizen (“fresh pursuit from one jurisdiction to another” would be an exception).

Rarely will police from one nation actually visit another—and then most frequently for the purposes of extradition. This requires extensive coordination, generally between local embassies and often through the various State Department and Foreign Ministries as well as respective Departments of Justice or Home Offices. Officers are almost always prohibited from carrying their weapons abroad.

However, there are instances where such extra-judicial cooperation does occur. For example, in the 1999 I LOVE YOU virus investigation, agents of the FBI were invited to the Philippines and worked hand-in-hand with the Filipino National Bureau of Investigation in Manila to identify and arrest Mr. Guzman, the perpetrator.

Q: How is a private sector company in a foreign country contacted whose computers/networks are involved?
A: There would be several ways to approach this, the most likely being to speak with their local representative. For example, if the local Microsoft office in Auckland were involved in an incident, U.S. investigators would most likely work the case through Microsoft Security in Redmond, Washington. This technique is generally successful. If investigators were dealing with a foreign corporation with no U.S. point of presence, things could be more difficult, but generally, investigators would either contact a law enforcement liaison in the foreign country or, in the absence of such a program, contact the company’s security or general counsel’s office. The other benefit of having a multinational corporation with a local presence is that court papers requesting information can be served on the local subsidiary. For example, if the FBI wanted something from Alcatel in France, it could theoretically serve papers on Alcatel in the U.S. to gain compliance. This technique works much of the time, but not always, depending upon the legal structure of the corporation and its relationship to the parent organization.

Q: How do you get the evidence physically transported?
A: Logs can be sent by CD, facsimile, e-mail (depending on size), or private carriers such as Federal Express, UPS, or DHL. It all depends. In extreme cases, an agent could be sent abroad to physically seize the data.

Q: What are chain-of-custody laws?
A: Chain-of-custody laws vary significantly by jurisdiction. One can avoid many of these issues, particularly if the case does not go to trial and the suspect pleads out. Also, defense counsel may stipulate to the provenance of the evidence. A problem can arise, however, if evidence is obtained in a manner inconsistent with national legal standards. For example, if the police in a foreign country beat a confession out of a suspect, it may not be admissible in court if that conduct violated the country’s legal standards.
Q: Where do the roles of law enforcement end and prosecution begin?
A: This depends entirely on the prosecuting agency and the nature of the case. Some jurisdictions, especially in the task force model, work hand-in-hand with prosecutors. In some countries, there may be only investigating judges that receive case referrals directly from the police. Ideally, prosecutors are involved early in the process; in reality, prosecutors tend to have even less experience with high-tech crime than do police officers, and many have little interest in learning. In the U.S., at the federal level, attorneys in the Department of Justice’s Computer Crime and Intellectual Property Section, the Computer Hacking and Intellectual Property units, and the Communications and Telecommunications Coordinators in various offices have specialized expertise and work closely with investigators.

Q: As a practical matter, what should a business or individual confronted with cybercrime do?
A: The U.S. DOJ/CCIPS website contains a wealth of useful information on how to report Internet-related crime, with questions and answers and lists of links depending on the type of crime. On February 12, 2002, in cooperation with CIO magazine, the FBI and USSS released the first set of officially sanctioned Cyberthreat Response and Reporting Guidelines.

B. THE REALITY: IMMEDIATE NEEDS

The creation of a global legal environment that eliminates obstacles in the investigation and prosecution of cybercrime is critical if the problem is to be addressed at a systemic level. By addressing the two overarching issues and ten priority concerns that were identified in the National Institute of Justice Report discussed in Part II above, as well as the ten principles:

---


enunciated in the UN General Assembly Resolution 55/63, nation states can significantly advance the ability of their law enforcement to respond to cybercrime. This process can be advanced through the assistance of industrialized nations and the donor community to sponsor projects designed to transfer knowledge and skills, develop cybercrime laws, and increase international coordination. Other stakeholders, such as NGOs, private sector companies, and academic institutions, also have roles:

- The international legal community can launch initiatives to assist developing countries in (a) drafting strong cybercrime laws and regulations; (b) ensuring the capacity to enforce such laws through the training of judges, prosecutors, and law enforcement personnel; and (c) helping them to participate in global discussions on ICT and cybercrime issues.
- Communication providers can offer assistance to providers in developing countries regarding data retention, data preservation, compliance with orders, and cooperation with law enforcement.
- Private sector companies can work with their governments to develop trust and advance information sharing. Business leaders have a valuable role to play in both setting an example regarding the security of corporate data and networks and in encouraging companies small and large to report security breaches to law enforcement.
- Multinational corporations can apply pressure on developing countries to make combating cybercrime a national priority.
- NGOs can assist in raising public awareness and influencing policy and legal developments.
- Academic institutions can work with developing countries and donor organizations to improve curricula and provide adequate training (whether by distance learning, scholarships, foreign internships, or traditional methods) to law enforcement, ICT and security personnel, engineers, public and private sector management, students, and the workforce.

IV. Conclusion

The emergence and rapid escalation of cybercrime has significantly impacted law enforcement’s ability to investigate and prosecute crimes. In addition to coping with the rapid technological advances associated with cybercrime, law enforcement increasingly has to deal with cyber evidence and ICT’s role in traditional crimes such as murder, rape,
the illegal sale of drugs, and child pornography. Governments must devote ongoing attention and resources to high-tech investigative and forensic training, the establishment of internal organizations, and active involvement on the international front.

Combating cybercrime also calls for a new partnership between the public and private sectors to enhance the ability of law enforcement to meet the challenge of high-tech crime. Such a partnership should be based on information sharing, cooperation, and joint work toward fostering global minimum standards. Numerous multinational organizations are addressing cybercrime, with the CoE, G-8, and UN in leadership roles. Despite these activities, however, international efforts lack coordination, and law enforcement continues to face barriers and procedural delays caused by inadequacies in legal systems and the lack of a global, harmonized legal framework. Industrialized nations and donor organizations can advance this process by helping developing countries enact cybercrime laws, establish needed government entities, and provide critical training. The private sector can also help through assistance provided by the legal community, communication providers, private sector companies, and nongovernmental organizations.
Search and Seizure

I. Introduction

Law enforcement agencies investigating cybercrime (as well as traditional crime) have at their disposal an array of investigative techniques for obtaining evidence. These include the interception or tracing of communications (both voice and data) by electronic means and the search for and seizure of digital evidence. Use of such techniques poses both legal and practical considerations. Government access to communications and stored data often involves an intrusion on privacy and, therefore, requires adherence to legal standards that balance the governmental interests in effective law enforcement with the widely accepted right to protection of privacy. In practical terms, the acquisition of electronic evidence poses unique challenges because the collection of digital evidence requires special care and expertise as compared with the seizure of paper-based evidence. This chapter outlines acceptable practices and practical considerations pertaining to seizure of stored data from computers. It also discusses the legal standards that relate both to the interception of communications and the search for and seizure of digital evidence.

In many countries, legal standards for government information gathering that is conducted in defense of the national security and in the pursuit of foreign policy interests (foreign intelligence wiretaps and other forms of foreign intelligence gathering) differ from the legal

1For example, in the United States, foreign intelligence and counterintelligence surveillance is governed by the Foreign Intelligence Surveillance Act, 50 U.S.C. Sections 1801–1863, http://www4.law.cornell.edu/uscode/50/1801.html. In Germany, Article 10 of the Basic Law stipulates that where an interception is undertaken for national
standards applicable to law enforcement. In this document, we focus only on standards and practices in the law enforcement sphere.

Generally, there is no single accepted best practice: Not only may best practices differ from country to country, but within countries that have federal systems, the state, provincial, or local authorities may adopt legal standards or practical methods that vary from those followed by the national government. Further, best practices change as technology changes. Nevertheless, both in terms of legal standards and practical considerations, there is a growing body of standards and acceptable practices, based on the real-world experiences of leading law enforcement agencies. Nations seeking to improve their response to cybercrime would benefit from adoption of these standards and practices.

A. CHAPTER OVERVIEW

This chapter addresses searches and seizures and other forms of law enforcement access to digital evidence, offering practical suggestions and summarizing legal standards. Part II provides an overview of the types of governmental actions discussed: real-time interception of communications, real-time interception of traffic data, immediate access to stored data by means of a search and seizure, and compelled disclosure of stored data by means of a subpoena. Part III addresses practical considerations for immediate seizure of digitally stored evidence. Part IV discusses legal considerations, beginning with an overview of the right to privacy and describing its application in judicial and statutory standards for live interception of communications and traffic data, for access to stored communications and traffic data, and for search and seizure of other stored data. Part V concludes with a discussion of the jurisdictional issues unique to cross-border searches and seizures.

II. Overview of Types of Search and Seizure

It is useful for analytical purposes to draw distinctions among the different means by which digital evidence may be collected. In this chapter, as in the law and procedures of many countries, the real-time interception of communications is distinguished from the search for and seizure of stored electronic data. In turn, distinctions are made

security purposes, the person affected need not be informed and recourse to the courts shall be replaced by a review of the case by bodies appointed by Parliament. See German Basic Law, http://www.oere.unibe.ch/law/the_basic_law.pdf.
between the seizure of the content of communications and the seizure of transactional or traffic data that do not reveal the substance or meaning of a communication.

A. REAL-TIME INTERCEPTION OF COMMUNICATIONS

One way of gathering evidence is to intercept information as it passes between two or more people or two or more computers. This is called wiretapping, eavesdropping, or "live interception." Under legal systems that have the concept of a "search and seizure" (for example, Canada, United States), live interception of the content of communications is considered to be a search and seizure within the protections of the Constitution. Under almost all legal systems, the interception of communications is considered a privacy intrusion of the highest order, requiring strict legal protections.

Some legal systems, such as that in the United States, distinguish between interception of communications that are in transit and access to communications that are held in storage by a service provider or by the intended recipient. In the United States, seizure in either case generally requires prior judicial approval under the highest standard in the Constitution for searches and seizures (the probable cause standard). However, if the government wants to listen to conversations in real time or read e-mails as the computer user is sending them, then it generally needs to obtain a wiretap order, which is subject under U.S. law to more stringent limitations than ordinary search warrants. If, on the other hand, the government wants to seize the unopened messages that have already been sent to a specific e-mail account or voice-mail storage, then it needs only obtain a search warrant. This still requires approval by a magistrate or judge under the Constitution's highest standard.

B. REAL-TIME INTERCEPTION OF TRAFFIC DATA

The law in several countries (including the United States and the United Kingdom) also distinguishes between the interception of the content of communications and the interception of only the transactional data or traffic data, which indicates the origin and destination of each communication. Equipped with the information identifying the origin

---

2As an example, consent to seizure is an exception to the requirement for judicial approval.
3Usually, a content interception also collects the traffic data associated with each communication: date, time, duration or size of the communication, and numbers or other information identifying the destination or origin of the communication.
and destination of communications, law enforcement officers can often obtain from service providers the names and addresses of the subscribers associated with those communications. Traffic data, especially when combined with such subscriber-identifying data, are both very useful to the investigative process and sensitive from a privacy standpoint, for they may reveal the patterns of a person’s associations, interests, and activities. For these reasons, interception of traffic data should be subject to legal controls. Still, under various legal systems, while the real-time interception of content requires the highest form of judicial approval, real-time interception of traffic data can be authorized under a lower standard. This distinction is based on the premise that traffic data, while sensitive, is less revealing than the content of communications. Definitions of traffic data, and how to distinguish between it and the content of communications, especially in the Internet context, vary from jurisdiction to jurisdiction.

C. IMMEDIATE ACCESS TO STORED DATA BY MEANS OF SEARCH AND SEIZURE

In contrast to the real-time interception of communications and associated traffic data, evidence can also be obtained while it is at rest or in storage. A classic law enforcement technique equally relevant in the digital age is the search and seizure of evidence—the entry by law enforcement officers into a home or office to search for and seize evidence of a crime or contraband. Again, in many legal systems, this is considered a privacy invasion of the highest order and requires in most instances prior legal approval, in many legal systems by a judicial officer, upon a showing by investigators of need and justification. Increasingly, in both cybercrime and ordinary criminal investigations, these searches involve—and sometimes focus largely on—the search for information stored in computers. Generally, the legal standards for a search of tangible items and digital evidence are the same, but the practical considerations are quite different.

4The European Court of Human Rights, for example, has stated, “By its very nature, metering is therefore to be distinguished from interception of communications. . . . The Court does not accept, however, that the use of data obtained from metering . . . cannot give rise to an issue under Article 8 [protecting the right of privacy]. The records of metering contain information, in particular the numbers dialed, which is an integral element in the communications made by telephone. Consequently, release of that information to the police without the consent of the subscriber also amounts, in the opinion of the Court, to an interference with a right guaranteed by Article 8.” Malone v. U.K., judgment of Aug. 2, 1984, Series A no. 82, 7 EHRR 14.
D. COMPELLED DISCLOSURE OF STORED DATA
BY MEANS OF A SUBPOENA

Sometimes law enforcement officers need to exert control over private premises and search for and seize evidence. This often occurs when the evidence sought is in the control of the suspected criminal, who would destroy it if given the chance. However, in other cases, when the information is in the hands of an innocent third party—such as a communications service provider or system administrator—the government most likely does not need to immediately secure the evidence and conduct its own on-the-spot search. It can rely instead on the record custodian to faithfully identify and turn over to the government any relevant information in its possession, which does not involve the kind of disruption entailed in a search and seizure. Still, such disclosures intrude upon the privacy interests of the record subject (the person to whom the information pertains) and normally require some form of independent approval and oversight. In these cases, the law enforcement agency does not need the power of the search warrant, but can use some other means to compel production of the information—a subpoena or court order, depending upon the legal system.

III. Practical Considerations for Immediate Search and Seizure of Digitally Stored Evidence

An investigator can follow all legal requirements, but if the evidence is not acquired fully, without damage, and in a way that provides assurance of its origin and integrity, a prosecution may fail. This section describes the practical considerations for the proper acquisition of digital evidence.

A. SCOPE

The prosecution of cybercrime—and increasingly of other crimes—necessarily requires the acquisition of digital evidence. There are at least three major ways to obtain electronic evidence. The first is to obtain a subpoena or court order directing a service provider, computer system operator, another business entity, or an individual to disclose stored computer data. The second is to enter premises under legal authority and search for and seize evidence on an electronic storage device or media such as a computer hard drive, compact discs (CDs), or diskettes. The third is through live interception of communications and/or traffic data via a wiretap, sniffer, or pen register or trap-and-trace device. Evidence may also be obtained
through other methods: for example, in undercover operations in which the target voluntarily, but unwittingly, communicates with a law enforcement officer, such as an officer posing as a little girl in a chat room in order to catch a pedophile.

B. OVERVIEW

In all criminal investigations it is necessary to acquire evidence. Investigators need to prove who did what, and how. In the cybercrime arena, these points are likely going to be proven, at least in part, by digital evidence. However, as in all criminal investigations, all forms of evidence may be relevant to a cybercrime investigation. Thus, the first rule of search and seizure is the collection of all relevant evidence, including nondigital evidence. For example, cyber evidence may make it possible to track an e-mail back to a particular computer at a particular time, but such information would be insufficient to successfully prosecute a crime without evidence showing who was at the keyboard at the time the e-mail was sent. This may be proven by traditional investigative techniques, including interviews and physical surveillance.

Second, because any search and seizure of evidence will have to follow the legal rules of the particular jurisdiction where the search is being conducted, it is important to fully plan the search before seeking the necessary authorization, to ensure that the approval obtained is consistent with the desired scope of the search.

Third, investigators need to be aware that digital evidence is, in many respects, fragile and easily corrupted. Because the collection of this evidence is different from the traditional collection of evidence, it must be obtained in a careful and thoughtful manner.

Evidence collection techniques constantly evolve for two reasons. First, legislators and courts may change the legal standards for search and seizure (1) to account for changes in the nature of criminal conduct, (2) in an effort to keep pace with technological changes, or (3) to ensure that there is the proper balance between accountability and privacy protection on the one hand and the interests of law enforcement agencies on the other hand to respond promptly and effectively to crime. Investigators need to keep current with the details of the legal standards. (For that reason, direct reliance on this publication is not recommended: Investigators must work with those familiar with the latest version of the law(s) affecting their activities.) Second, evolving technologies greatly affect the best practices in this area. Law enforcement agencies and private companies are constantly developing new evidence recovery tools, just as criminals are constantly taking
advantage of new technologies to intercept, store, and transmit information. Investigators need to keep abreast of the latest developments in computer forensic techniques.

C. METHODOLOGIES FOR COLLECTION OF DIGITALLY STORED EVIDENCE

Evidence can be acquired “live” (as it is being transmitted) or it can be collected from electronic storage. In this section, we focus on the latter, in particular on searches of computers and computer systems that have been or will be turned off prior to acquisition of the digital evidence. Basic, best practices in this area include the following:

1. Evaluate the Target

- Through investigation, including physical surveillance, interviews, informants, or live interception, identify the type of computer and whether it is a stand-alone system or attached to a network.
- Attempt to determine how many people in the home or business have access to the computer system.
- Determine whether the target has Internet access from the target computer and the method of access (that is, dial-up, cable, DSL, and so forth).
- Ascertain whether you will need a warrant. In the United States, most searches and seizures of computer evidence require a search warrant.
- If a search warrant or other prior approval is needed, pay close attention to the scope of the search. Some systems may require separate legal authority for the seizure of evidence and the subsequent forensic examination of the evidence. Thus, for example, if the forensic examination will be conducted by an agency other than the one doing the search, it may be necessary in your search warrant application to seek and obtain explicit authority for that agency to examine the evidence.
- Be familiar with the types of potential evidence.
- The most important piece of hardware is the case or tower, otherwise known as the computer itself, because it contains the hard drive where most of the data is stored.
- Unless the monitor, keyboard, and mouse are instrumentalities of the offense, the seizure of these items may not be necessary because they probably do not contain any usable evidence. Nevertheless, they should be seized in order to ensure that all relevant evidence may be properly examined.
Do not forget to seize all other relevant media, including printers; scanners; external modems; external storage devices (CD drives, zip drives, tape drives, external hard drives, and so forth); removable media (floppy disks, compact disks, zip disks, and the like); computer manuals, software, digital cameras and accessories; handwritten notes and notebooks containing names and/or e-mail addresses, website addresses, passwords, and so forth; and Personal Data Assistants (PDAs). Valuable evidence often is obtained from these items.

2. Develop a Plan

Planning is critical in computer and electronic evidence searches.

- Develop an operations plan that includes all agents involved in the search and their responsibilities: the entry team, uniformed officers to secure the people and scene, computer expert, and others.
- Brief the search team and ensure that each actor is familiar with his/her assignment.
- Precautions normally taken to ensure officer safety during a search and seizure should also be taken in conducting raids for computer evidence.

3. Execute the Plan

- Once entry has been accomplished, secure the scene and remove any individuals from the proximity of the computer or power sources.
- Do not allow any unauthorized or untrained personnel to touch the computer or any computer system equipment.
- To the extent legally permissible, interview both potential defendants and innocent parties regarding password protection devices, encryption programs, or any special program that the computer system or individual files may require. Check the area for remote infrared or voice-activated devices. These devices, while rare, could inadvertently start a covert process of data destruction.

The risk of businesses losing their ability to remain operational if computer assets and data are seized is less of a concern when investigators merely make copies of the data and software and leave the assets alone. However, this may not be feasible when forensic evidence needs to be obtained from the hard drive and memory of the computer.
4. Preserve the Evidence and Prepare It for Transport

Photograph the room in which the computer is located, any images on the screen, the computer, peripheral devices, cabling, and other peripherals, and the area surrounding the computer, media, papers, manuals, access codes, passwords, and so forth.

- It is VERY important that the power source of the computer be terminated in such a way as to not corrupt any evidence. When doing so, DO NOT shut the system down using the operating system, or by way of the power switch on the computer. If you can determine that the cord from the computer runs directly to the wall socket, then pull the plug from the wall. Otherwise, remove the power cord directly from the back of the computer.
- Insert a prepared seizure diskette or wiped nonsystem disk into each drive bay and seal with evidence tape.
- If the computer is connected to a modem line, disconnect the cable at the wall. Test for dial tone with a telephone handset and make a written note if the telephone line is operational at the time of the search.
- Remove cover and photograph internal components and jumper settings.
- Disconnect power to any hard drive.
- Seize and record evidence authorized to be seized by the search warrant or consent.
- Tag and label all cables and note connections to peripheral devices.

---

6The best practices set forth in this document are very basic in nature. Very experienced forensic examiners may want to obtain evidence from a computer prior to removing its power. For example, all information in the random access memory (a.k.a. RAM) will be lost forever when the computer is turned off. However, since there is great risk of altering the evidence under this scenario, only the most experienced investigators should attempt to obtain any information from a “live” system.

7Some computers may be equipped with a device known as an uninterruptible power supply. This is, essentially, a battery that automatically supplies power to the computer if the normal power source is terminated (that is, loss of power during thunderstorm and the like). While this, in and of itself, is not problematic, the real issue is that some of these uninterruptible power supplies will automatically shut the computer down using proprietary software. Naturally, this process could change the data on the hard drive and could, therefore, create an issue as to the reliability of the evidence seized.

8A “wiped” disk means it has no data on it. This would most likely be a disk with all ones or all zeros to assure that the computer did not obtain any data from the disk while in storage. “Nonsystem” means that the disk does not contain an operating system so that even if the machine were turned on, it likely would not boot while such a disk were within its floppy drive.
Tape and label any empty ports or slots not in use.
Make sure to take photographs that clearly display the wiring configurations before disassembling the computer system.
Carefully label, log, package, and prepare all evidence seized.
When transporting and storing evidence, ensure that all components and media are kept away from two-way radios and any magnetic devices.

5. Conduct the Forensic Examination

A forensic examination of electronic evidence cannot be conducted without background from the investigating officer, a copy of the search warrant, and input from prosecuting authorities regarding the scope of the search sought. This is because forensic examiners of digital evidence are conducting a search. In order to properly execute the search, the examiner must have the search warrant, if there is one, and he or she must read it in order to ascertain the parameters of the search. The investigator should outline exactly what is sought: for example, text strings or images, spreadsheets, chat logs from a particular chat room, and the like. Particularly in cases with a large volume of evidence, it is essential for the forensic examiner, the investigating officer, and the prosecutor to come to agreement about the extent of the search required. Looking at gigabytes of data can take weeks or months and may not always be necessary.

D. BEST PRACTICES GUIDES AVAILABLE

There are a few guides available that outline procedures for seizing computers and electronic hardware. Guidelines for seizing and for evaluating Internet- and network-related records and logs are more difficult to find.

1. United States

   (i) United States Government

   The United States Government has developed several useful resources:

   - *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, U.S. Department of Justice, Computer Crime and Intellectual Property Section, Criminal Division, July 2002 (http://www.cybercrime.gov/s&smmanual2002.htm): state, local, and international law enforcement must bear in mind that the U.S. government developed this guide for federal law enforcement officers. Therefore, any legal requirements unique to the state or local jurisdiction must be considered.


(ii) State Government
Three states have developed guidelines for computer and electronic evidence search and seizure:

- Connecticut Guidelines for Searching and Seizing Computer Systems and Electronic Evidence, State of Connecticut Division of Criminal Justice and Department of Public Safety, 1999. (Available by request from Computer Crimes and Electronic Evidence Unit, 278 Colony Street, Meriden, CT 06451.) These guidelines mirror the federal guide, addressing state issues such as obtaining Internet subscriber information by search warrant and state evidentiary rules. The document provides an overview and discussion of pertinent state and federal statutes and cases.


- New Jersey Computer Evidence Search and Seizure Manual, State of New Jersey, Department of Law and Public Safety, Division of Criminal Justice (http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf): a comprehensive guide that covers search warrants, warrantless searches, wiretap authorizations, forensic examination,

---

9Also of interest may be the training programs offered by the Federal Law Enforcement Training Center for Seized Computer Evidence Recovery Specialists; See http://www.treas.gov/fletc/ffl/scers.htm.
and legal considerations relating to admitting electronic evidence in court.

(iii) Local Prosecutors
At least one local prosecutor’s office in the United States has prepared a guide:

- Computer Searches, Alameda (California) District Attorney (http://www.co.alameda.ca.us/da/pov/web.htm).

(iv) Others
The ABA has also produced a guide:


2. Canada

Canadian information is available at:


3. Industry Bodies

An industry body that has prepared a best practices document includes:

- LINX, Best Current Practice on User Privacy, Version 1.0—May 15, 2001 (http://www.linx.net/noncore/bcp/privacy-bcp.html): the London Internet Exchange (LINX) has served as a forum for discussion with representatives of Government and other bodies on practical questions regarding interception of communications and disclosure of communications data on the Internet, to ensure that legislation and resulting actions are realistic and reasonable for LINX members, and to protect the privacy interests of their subscribers.

4. Council of Europe

The Council of Europe has also issued recommendations:

- Council of Europe Committee of Ministers Recommendation No. R (95) 13 of the Committee of Ministers to Member States
E. SUMMARY OF PRACTICAL CONSIDERATIONS

This section briefly covered the preferred practices for collection of digital evidence from computers. The law will dictate the proper practices for collection of digital evidence. Likewise, advances in technology are likely to change those procedures as well. Nevertheless, there are certain things that probably will not change. The target must be evaluated and a plan of attack must be formulated. The plan should then be executed, and the evidence evaluated and preserved for future use. In developing the plan, it is imperative that the investigator know the local laws as well as the technologies involved. For example, is this going to be a capture of live information, or is it going to be a seizure or imaging of a hard drive? Finally, following best practices likely will be the best plan to attain the goal.

IV. Legal Considerations

A. LEGAL STANDARDS OVERVIEW

1. International Human Rights Protection of Privacy

Absent consent or access to public communications, government interceptions of communications (and traffic data) and government seizures or compelled disclosures of data in the hands of businesses and individuals constitute an intrusion on personal privacy. Under most legal systems, such intrusions are permissible, but only in accordance with clear standards in the law, requiring justification and prior independent approval, often of a judge. Legal standards limiting the circumstances and procedures for interception, search, and seizure are evolving, but governments and international human rights bodies are paying increasing attention to the procedures.

The right to privacy is widely recognized as a fundamental human right under various human rights instruments, including the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the European Convention on Human Rights, and the American Convention on Human Rights. Article 12 of the Universal Declaration of Human Rights states: “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right
to the protection of the law against such interference or attacks.”

Likewise, Article 8 of the European Convention on Human Rights (ECHR) provides: “Everyone has the right to respect for his private and family life, his home and his correspondence.” The provisions of the European Convention are binding on all 44 Member States belonging to the Council of Europe.

These human rights instruments normally permit government searches and seizures, pursuant to strict controls. Thus, Article 8 of the ECHR provides: “There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”

2. National Constitutions

Nearly every country in the world includes a right of privacy in its Constitution or other basic law. These provisions normally include rights of inviolability of the home and secrecy of communications. For example, the Fourth Amendment to the U.S. Constitution provides “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.” Article 10 of the German Basic Law provides: “The privacy of letters as well as the secrecy of post and telecommunication is inviolable.” Most recently written constitutions include specific rights to control one’s personal information in the hands of third parties, such
as businesses. For example, the new Constitution of Spain of 1978, the new revised Constitution of Portugal of 1982, the Constitution of the Netherlands of 1983, and the new Constitution of Brazil of 1988 even contain specific safeguards protecting their citizens’ privacy against the incursions of modern computer technology. In many countries in which privacy is not explicitly recognized in the Constitution, the courts have found that right in other provisions.

As with the international human rights instruments, these constitutional provisions normally recognize that intrusions may generally be made only upon adherence to strict procedures. For example, the Fourth Amendment to the U.S. Constitution goes on to state, “and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the person or things to be seized.” Paragraph 2 of Article 10 of the German Basic Law states, “Restrictions may only be ordered pursuant to a statute.”

B. JUDICIAL AND STATUTORY STANDARDS FOR LIVE INTERCEPTION OF COMMUNICATIONS AND TRAFFIC DATA

Given the grave privacy intrusion that live interception represents, strict legal standards apply to its authorization. Based upon developing national and international standards, it is possible to identify certain common elements that should govern any legal system for live interception:

- Approval should be obtained from an independent official (preferably a judge), based on a written application and manifested in written order.

- Approval should be granted only upon a strong factual showing of reason to believe that the target of the search is engaged in criminal conduct and that the technique is especially needed.
(that is, interception is reserved for serious offenses and used only when other less intrusive techniques will not suffice).

- Each surveillance order should cover only specifically designated persons or accounts; generalized monitoring should not be permitted.
- The rules should be technology neutral: All one-to-one communications are treated the same, whether they involve voice, fax, images or data, wireline or wireless, digital or analog.19
- The scope and duration of the interception is limited, and in no event does the surveillance extend longer than is necessary to obtain the needed evidence.
- In criminal investigations, all those who have been the subject of an interception should be notified after the investigation concludes, whether or not charges result.
- Personal redress or suppression of evidence at trial is provided for violations of the privacy standards.20

1. Europe

As noted above, Article 8 of the European Convention on Human Rights provides that everyone has the “right to respect for his private . . . life . . . and his correspondence,” subject only to such interference “as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others.”21 This provision serves, in addition to national constitutions, as the fundamental source of limitations on government search and seizure throughout the 44 nations that are members of the Council of Europe (CoE) and as an important source of international norms.

The CoE Convention on Cybercrime specifically requires countries bound by the European Convention to adhere to its obligations in the implementation and application of the search and seizure powers

---

19Under U.S. law, a limited exception exists in 18 U.S.C. Section 2516 that allows the government to intercept voice communications only for certain enumerated felonies, while allowing the interception of electronic communications for any federal felony.

20U.S. law allows for both personal redress against individuals who violate the privacy standards and the suppression of evidence in legal proceedings.

contemplated under the Convention for the obtaining of electronic evidence. Article 15 of the Cybercrime Convention provides:

1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, . . . and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2. Such conditions and safeguards shall, as appropriate in view of the nature of the power or procedure concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation on the scope and the duration of such power or procedure.22

The basic privacy principle in Article 8 of the European Convention on Human Rights has been given greater definition by the European Court of Human Rights (ECtHR), which has defined a set of minimum standards governing electronic surveillance. The case law of the ECtHR is today one of the most important sources of international norms on live search and seizure of communications. The Court, applying Article 8 of the European Convention, has laid down the following minimum standards:

- First, the surveillance measures must have a basis in domestic law, which normally means that the surveillance power must be embodied in legislation.
- Second, the requirements of the Convention refer to the quality of the law in question, requiring that it:
  - Be accessible to members of the public;
  - Be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in, and conditions on, which public authorities are empowered to resort to such measures;

---

- Have clear, detailed rules, so that citizens are able to foresee its consequences, especially as the technology available for use is continually becoming more sophisticated;
- Be sufficiently precise to give the individual adequate protection against arbitrary interference; and
- Be compatible with the rule of law.23

The Court has expressed a strong preference for supervision by an independent judge, 24 but in all instances oversight and control of surveillance measures must be exercised by independent authorities vested with sufficient powers and competence to exercise effective and continuous control.

While the Court has never exclusively defined the minimum elements of a surveillance law, it has endorsed the following standards in ruling on wiretap laws:

- The legislation limits surveillance only to the investigation of specified, serious crimes.
- Surveillance may be ordered only if the establishment of the facts by other investigative means is without prospect of success or would be considerably more difficult.
- Surveillance may cover only the specific subject or other defined categories of persons.
- Surveillance may be ordered only upon written application giving reasons and setting forth facts justifying the intrusion.
- The length of time for which the surveillance can be conducted is limited (for a maximum of three months) and may be renewed only on fresh application.
- The surveillance must be conducted in such a way as to reduce the intrusion on privacy to an unavoidable minimum necessary to obtain the needed evidence.
- The measures must immediately be discontinued as soon as the preconditions for surveillance cease to exist or the evidence has been obtained.
- The enabling legislation should describe the use to which seized or intercepted material could be put; information obtained for criminal investigative purposes may not be used for other ends.

---

24See Kopp, cited above; Klass v. Germany, Sept. 6, 1978, 2 EHRR 214 (“The Court considers that, in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge.”).
The law specifies procedures for drawing up summary reports for a judge’s review and precautions to be taken in order to permit inspection of the recordings by the judge and by the defense.

- Recordings and transcripts must be destroyed as soon as they are no longer needed to achieve the required purpose, for example, if charges are not brought or the accused is acquitted.\(^2^5\)

National laws incorporating these standards include those of Germany\(^2^6\) and France.\(^2^7\)

2. United States

(i) General\(^2^8\)

Under the Fourth Amendment to the U.S. Constitution, the government generally must obtain a written court order before its agents can intercept the content of communications.\(^2^9\) (Failure to do so


\(26^\text{See Section 100 of the Criminal Procedure Code (Strafprozeßordnung, StPO), an English version of which is online at http://www.iuscomp.org/gla/statutes/StPO.htm.}

\(27^\text{See Article 100 of France’s Code of Criminal Procedure, online at http://www.legifrance .gouv.fr/html/frame_codes1.htm.}

\(28^\text{See generally Fishman & McKenna, Wiretapping and Eavesdropping, Second Edition (1995).}

\(29^\text{This principle was established by the U.S. Supreme Court in the landmark 1967 cases of Berger v. New York, 388 U.S. 41 (1967), and Katz v. United States, 389 U.S. 347 (1967).}

There are certain exceptions to the court order requirement. Pursuant to 18 U.S.C. Section 2518(7), the Attorney General may authorize interception for up to 48 hours if he or she determines that an emergency situation exists in which a person’s life or health is threatened, national security may be compromised, or the activities concern organized crime. The government must make a full written request to a judge within two days or discontinue the wiretap.

Another exception relates to interception where one of the parties to the communication consents to it being recorded. That type of recording is considered a “consent” recording and, under federal law in the United States, no judicial order is needed. 18 U.S.C. Section 2511(2), the text of this provision can be found at http://www4.law.cornell.edu/uscode/18/2511.html. The legality of consent recordings varies from jurisdiction to jurisdiction even within the United States. For instance, New York State permits them. Pennsylvania permits them but requires the Attorney General of the State or one of his or her designees to interview the person making the recording personally in order to determine that consent was voluntarily given. A minority of other states prohibits them completely, requiring, in general, that all parties to a conversation must consent to its being recorded. Most recently, 18 U.S.C. Section 2511(2)(i) was added to permit the owners or operators of computers to authorize law enforcement to intercept the communications of a computer trespasser.
may prevent the use of evidence in a criminal proceeding.) The federal wiretap legislation was first enacted in 1968.\textsuperscript{30} It generally prohibits all interception of communications, by private parties or by the government, unless authorized by a court order or permitted by an exception. It was amended in 1986 to take into account technological advancements such as wireless communications and communications over computer networks.\textsuperscript{31} As amended, the law generally requires a judicial order for interception of all wire, oral, and electronic communications.\textsuperscript{32}

The process for obtaining an eavesdropping warrant involves several steps. First, the Attorney General of the United States or another senior official must personally authorize a federal law enforcement agent to apply for the court order.\textsuperscript{33} The agent, in turn, submits to a federal judge a detailed, sworn affidavit laying out the facts that justify the issuance of the warrant. The application must also provide a description of the facility to be intercepted, such as the telephone number in the case of wiretaps, the e-mail account for data intercepts, or the address and room where a bug will be located. The agent must also explain what other investigative tools he or she has used, if any, and why they have not been or are not likely to be successful.\textsuperscript{34}

The application is submitted to a judge. This judge can issue an order authorizing interception only if he or she finds, based on the government’s factual assertions, “probable cause to believe” that: (1) the target whose conversations will be intercepted is committing, has committed, or is about to commit a crime; (2) the target will engage

\textsuperscript{30}18 U.S.C. Sections 2510–2522; the text of these provisions can be found at http://www4.law.cornell.edu/uscode/18/2510.html. This legislation governs the U.S. federal government. The legislation authorized the states to enact their own wiretap statutes, and a number of states have done so. Pursuant to the Supremacy Clause of the U.S. Constitution, however, the states cannot enact legislation less protective of privacy than the federal law. State laws can, however, place stricter requirements on eavesdropping by state and local officials. See also 18 U.S.C. Section 2516(2); the text of this provision can be found at http://www4.law.cornell.edu/uscode/18/2516.html.

\textsuperscript{31}The law was further amended in 2001, following the September 11, 2001, attacks, by the \textit{USA PATRIOT Act}, but the basic standards for interception described here were not altered. The text of the \textit{USA PATRIOT Act} may be found at http://thomas.loc.gov/cgi-bin/bdquery/z?d107:HR03162:|TOM:/bss/d107query.html.

\textsuperscript{32}An “electronic communication” is defined as any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part through a wire, radio, electromagnetic, photoelectronic, or photo-optical system.18 U.S.C. Section 2510(12).

\textsuperscript{33}18 U.S.C. Section 2516(1).

\textsuperscript{34}18 U.S.C. Section 2518(1)(a)-(c), the text of this provision can be found at http://www4.law.cornell.edu/uscode/18/2518.html.
in conversations that provide evidence about that crime; and (3) the target will do so over the telephone or other facility that is at issue.35 Orders for interception of voice communications can be issued only for the investigation of certain serious crimes enumerated in the statute. In all cases, the judge must be convinced that the agents have tried to obtain evidence through other means and have been unsuccessful or that attempting to use traditional law enforcement tools, such as undercover officers, would be too dangerous or would not yield the necessary proof.36

The statute also authorizes the judge to direct the government to make periodic progress reports to him or her about the status of the investigation during the period of interception.37 The statute limits the effective period of the warrant to 30 days, subject to renewal upon approval of the court.38 Except in special circumstances, the order must specify the place where, or the facility from which, the interception will be accomplished. Agents conducting a wiretap are required to do so in a way that minimizes the interception of innocent conversations. After the surveillance ends, the statute requires the court to notify the target of the surveillance.

(ii) Real-Time Interception of Traffic Data

U.S. federal law separately provides for the live interception of transactional data, such as the interception of numbers identifying the destination of outgoing calls or Internet communications (carried out by a device or process known in the United States as a “pen register”) and the interception of the data identifying the origin of incoming communications on the surveilled line or account (carried out by “trap-and-trace” devices).39 Interception of this data requires a judicial order, but the standard is not as high as that for content interception; the court needs only to find that the government has certified that the information sought is relevant to an ongoing criminal investigation. Traffic data can be intercepted in the investigation of any crime.

3518 U.S.C. Section 2518(3)(a), (b), (d).
3618 U.S.C. Section 2518(3)(c), the text of this provision can be found at http://www4.law.cornell.edu/uscode/18/2518.html.
3718 U.S.C. Section 2518(6).
3818 U.S.C. Section 2518(1)(d). In requesting extensions, the government must make the same type of written application as when applying for the first warrant and must include a summary of what was learned as a result of the prior interception. 18 U.S.C. Section 2518(1)(f).
3918 U.S.C. Sections 3121–3127, the text of these provisions can be found at http://www4.law.cornell.edu/uscode/18/3121.html.
Interceptions can run only for 60 days, subject to extension by order of the court. While the legislation was amended in 2001 to make it clear that it encompassed traffic data for Internet communications, the dividing line between content and noncontent remains unclear.

3. Canada

(i) General

The key limitation in Canada on the power of search and seizure is Section 8 of the Canadian Charter of Rights and Freedoms, which states: “Everyone has the right to be secure against unreasonable search or seizure.” The Supreme Court of Canada has held that surreptitious electronic surveillance constitutes a search or seizure within the meaning of Section 8. As a result, the interception of private communications must be authorized in accordance with the Criminal Code of Canada and must otherwise be considered “reasonable.” Among other things, this means that the interception must generally be authorized by a court. The procedure for applying for such authorization and the standard for authorizing a request for interception are set out in Part VI of the Criminal Code and summarized briefly below.

Part VI of the Criminal Code makes it an offense to willfully intercept “private communications” by means of any “electro-magnetic, acoustic, mechanical or other device” and outlines the circumstances in which the government or other parties can intercept, along with the process for obtaining authorization. Another section of the Criminal

---

40Canadian Charter of Rights and Freedoms, http://laws.justice.gc.ca/en/charter/. Evidence obtained through an unreasonable search or seizure (or through any other breach of the charter) must be excluded if its admission would “bring the administration of justice into disrepute.” Canadian Charter, Section 24(2). At the same time, if admitting the evidence would not bring the administration of justice into disrepute, the evidence may be admitted even if it was obtained through an unreasonable search or seizure.


42“Private communication” means “any oral communication, or any telecommunication”; “intercept” includes “listen to, record or acquire a communication or acquire the substance, meaning or purport thereof”; and “electro-magnetic, acoustic, mechanical or other device” means “any device or apparatus that is used or is capable of being used to intercept a private communication”; Criminal Code of Canada, Section 183. The Criminal Code of Canada is online at http://laws.justice.gc.ca/en/C-46/index.html.

43Intercepting a private communication without proper authorization and without falling into one of the exceptions set out in Part VI constitutes an indictable offense, punishable by a term of up to 5 years imprisonment. Criminal Code of Canada, Section 184.
Code makes it an offense to unlawfully use or disclose an intercepted private communication.\(^{44}\) To fall within the scope of either of these sections, the communication must be made such that the originator had a reasonable expectation that it would not be intercepted.\(^ {45}\) As a result, assessing whether a given technology affords users a reasonable expectation of privacy is important.

\section*{(ii) Application for Authorization}

The application for authorization must be made (1) in writing, (2) to a judge, and (3) accompanied by an affidavit sworn on information and belief.\(^ {46}\) The affidavit must set out the facts on which the application is based, the type of private communication to be intercepted and, if known, the identity of the persons whose communications are to be intercepted. It must also provide a general description of the place where the private communications are to be intercepted (if known), the proposed manner of interception, and the period for which the authorization is requested. It must describe the necessity of interception as an investigative technique by specifying whether other investigative procedures have been tried and failed, why it appears they are unlikely to succeed, or why it appears that the matter is so urgent that it would be impractical to use other means of investigation.\(^ {47}\) Finally, the affidavit may also provide a history of any prior applications, including any unsuccessful applications or applications that were withdrawn.

\section*{(iii) Standard for Judicial Authorization}

Before a judge may issue an authorization to intercept private communications, the judge must be satisfied of two things:\(^ {48}\)

\begin{enumerate}
\item that granting the authorization would be in the “best interests of the administration of justice”\(^ {49}\) and
\item that this means of investigation is necessary.
\end{enumerate}

\begin{footnotes}
\item[44] Criminal Code of Canada, Section 193.
\item[45] Criminal Code of Canada, Section 183 (definition of “private communication”).
\item[46] The process for applying for such authorization is set out in Criminal Code of Canada, Section 185.
\item[47] This necessity requirement, however, does not apply when the offense is one of several related to criminal organizations.
\item[49] According to the Canadian Supreme Court, this prerequisite imports a minimum requirement that there be reasonable and probable grounds to believe that an offense has been or is being committed and that the authorization will afford evidence of the offense.
\end{footnotes}
In terms of content, the authorization must describe (1) the offense in respect of which the authorization to intercept is given, (2) the type of communication that may be intercepted, (3) the identity of the persons, if known, whose private communications are to be intercepted, (4) the place of interception, if a general place can be provided, (5) the manner of interception, and (6) the period for which the authorization is valid (not to exceed 60 days). The judge may also impose such terms and conditions as he or she believes advisable in the public interest.50

(iv) Other Provisions
The interception provisions in Part VI of the Criminal Code also address a number of related issues. Section 186, for example, imposes strict limits on when a judge may grant an authorization in relation to the home or office of a solicitor or any other place ordinarily used by solicitors to consult with clients. It also permits the Solicitor General or Attorney General to designate who may make the authorized interception; stipulates that an authorization to intercept includes the authority to install, maintain, or remove the interception device covertly; provides for renewals of authorizations; and outlines the requirements for obtaining a renewal. Section 184.2 allows police to obtain court authorization where one of the parties to the communication consents to the interception and sets out the requirements for the application, the criteria for granting the authorization, and the terms to be included in such authorizations.

(v) Interception without Authorization
In addition to intercepting private communications pursuant to an authorization, there are several instances in which authorities may intercept such communications without authorization. An agent of the state may intercept a private communication without authorization where the interception is made with the consent of one of the parties to the communication and the purpose of the interception is to prevent bodily harm.51 A peace officer may also intercept without authorization if (a) the officer believes that the matter is so urgent that an authorization could not, with reasonable diligence, be obtained in time; (b) there are reasonable grounds to believe that the interception is immediately necessary to prevent an unlawful act that would cause

50Section 186(4) of the Criminal Code of Canada sets out the terms that must appear in all authorizations, but it also provides a general power to impose other terms and conditions the judge considers advisable in the public interest.
51Criminal Code of Canada, Section 184.1.
serious harm to a person or to property; and (c) one of the parties to the communication is the intended victim or the person who would commit that act.52

C. JUDICIAL AND STATUTORY STANDARDS FOR ACCESS TO STORED COMMUNICATIONS AND TRAFFIC DATA: THE U.S. MODEL

1. General

As previously noted, laws may treat live interception differently from access to stored wire and electronic communications. This is the case in the United States, where access to stored communications is governed by a chapter of the code entitled “Stored Wire and Electronic Communications and Transactional Records Access,” enacted as part of the Electronic Communications Privacy Act of 1986 (ECPA).53 This law sets forth the standards for governmental access to content and noncontent records associated with “electronic communications” in “electronic storage.” These particular terms were defined in ECPA.54 Digital evidence not within these definitions is not covered by ECPA and its seizure is regulated by general constitutional principles set by the courts. This discussion focuses on the U.S. federal law, although most U.S. states have local or state legislation applicable to local police

---

5318 U.S.C. Sections 2701–2711; the text of these provisions can be found at http://www4.law.cornell.edu/uscode/18/2701.html.
5418 U.S.C. Section 2510 contains relevant definitions:

“Electronic communication” means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system that affects interstate or foreign commerce, but does not include (a) any wire or oral communication, (b) any communication made through a tone-only paging device, (c) any communication from a tracking device, or (d) electronic funds transfer information stored by a financial institution in a communications system used for electronic storage and transfer of funds.

“Electronic storage” means (a) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof, and (b) any storage of such communications by an electronic communication service for the purposes of backup protection of such communication.

“Contents,” when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication.

See also 18 U.S.C. Section 2711; the text of this provision can be found at http://www4.law.cornell.edu/uscode/18/2711.html.
that, in large part, mirrors ECPA. Finally, it must be stressed that while the provisions of the law that govern access to stored e-mail are different from those that govern live interception, access to stored e-mail still requires in most cases a judicial warrant issued under the highest constitutional standard.

2. Standards for Disclosure

(i) Voluntary Disclosures
ECPA protects the privacy of e-mail and other stored electronic communications. Generally, providers of public communication services cannot disclose the contents of customer communication. Providers may disclose contents to the intended recipient, with the consent of the originator or recipient, or when necessary to preserve the “rights or property” of the provider. Providers of such services may also voluntarily reveal the contents of communications to law enforcement (1) if the communication was inadvertently discovered by the service provider and it appears to be pertinent to the Commission of a crime, or (2) if the provider “reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay.”

Noncontent records (for example, subscriber name and address) are treated differently. Providers may disclose such records to any person except a governmental entity for any reason, or no reason at all. On the other hand, providers may voluntarily disclose such records to the government, including law enforcement: (1) with the consent of the subscriber; (2) as may be necessary to protect the provider’s rights or property; or (3) if the provider believes that there is an emergency involving “immediate danger of death or serious physical injury.”

(ii) Compulsory Disclosures
Service providers can be compelled to disclose to the government e-mail and other electronic communications of their subscribers.

55The USA PATRIOT Act of 2001 made various changes to ECPA. Many of the corresponding state laws have not been changed to correspond with the Federal statute. Thus, in certain cases, state investigations requiring access to such data must be conducted in a fashion differently from portions of corresponding federal investigations.
5618 U.S.C. Section 2702(a); the text of this provision can be found at http://www4.law.cornell.edu/uscode/18/2702.html.
5718 U.S.C. Section 2702(b).
5818 U.S.C. Section 2702(b)(6).
5918 U.S.C. Section 2702(c).
6018 U.S.C. Section 2703; the text of this provision can be found at http://www4.law.cornell.edu/uscode/18/2703.html.
Generally, disclosure of the contents of communications is split into two different categories. The first deals with contents of a wire or electronic communication in “electronic storage” for 180 days or less, if unopened by the recipient. In such cases, law enforcement must use a search warrant. Second, if the unopened e-mail has been in electronic storage more than 180 days, law enforcement can use a subpoena, a court order, or a search warrant.\(^{61}\) If a search warrant is used in either case, no notice need be provided to the addressee or subscriber. If the government uses an administrative subpoena, grand jury subpoena, or court order (not a search warrant), it must provide prior notice to the subscriber unless doing so would seriously jeopardize the investigation, in which case notice can be delayed.\(^{62}\) These provisions apply only to content (the message part of an e-mail or the subject line), not for associated noncontent records, such as transactional data and subscriber information. Transactional (traffic) data is data that indicates the source or destination of a communication and requires a specific court order\(^ {63}\) or search warrant. Subscriber information requires only a subpoena but can also be obtained with a court order or search warrant.

Disclosure of noncontent records or traffic data is also divided into two categories depending on the exact type of information sought. Generally, the government may use a subpoena to require disclosure of noncontent records comprised of name, address, local and long-distance telephone connection records, records of session times and durations, length of service, types of service utilized, any temporarily assigned network addresses, and means and source of payment.\(^ {64}\) Notice is not required for these records.\(^ {65}\)

However, to obtain more detailed traffic data—the specific addressing information (that is, the “To” and “From” fields)—the governmental entity must obtain a court order based on specific facts showing that there are reasonable grounds to believe the information sought is relevant and material to an ongoing criminal investigation.\(^ {66}\) The service provider may challenge such court order if it promptly

\(^{61}\)18 U.S.C. Section 2703(a), (b).

\(^{62}\)See generally 18 U.S.C. Sections 2703(b), 2705(a); the text of this provision can be found at http://www4.law.cornell.edu/uscode/18/2705.html.

\(^{63}\)18 U.S.C. Section 2703(d); the text of this provision can be found at http://www4.law.cornell.edu/uscode/18/2703.html.

\(^{64}\)18 U.S.C. Section 2703(c)(2). State laws may not cover the same categories of subscriber records.

\(^{65}\)18 U.S.C. Section 2703(c)(3).

\(^{66}\)18 U.S.C. Section 2703(d).
files a motion to quash. Generally, this intermediate provision will be utilized in initiating investigations where there may not be quite enough evidence for probable cause, but the government still has some information to show the court. These “2703(d)” orders can be of particular value in cybercrime investigations where the governmental entity may need additional information in order to obtain a search warrant.

Because stored communications or transactional records are likely to be deleted from the logs of service providers after only a few days, the government may order the preservation of the information for up to 90 days. This section allows the government to request providers to preserve the existing records until it obtains the proper legal documents to actually obtain the records.

D. JUDICIAL AND STATUTORY STANDARDS FOR IMMEDIATE SEARCH AND SEIZURE OF STORED DATA: THE CANADIAN MODEL

The seizure of stored evidence (as opposed to communications) may be subject to different rules than those applicable to the interception of communications. In both cases, a privacy interest is at stake, and strict procedures need to be adhered to. These procedures may be found in both statutes and court decisions. In this section, as one example, we describe the statutory and judicial rules of Canada for seizure of stored evidence.

1. Constitutional and Judicial Considerations

As noted above, the key limitation on the power of search and seizure in Canada is Section 8 of the Canadian Charter of Rights and Freedoms, which states: “Everyone has the right to be secure against unreasonable search or seizure.” Under Canadian law, a search is considered

---

67A motion to quash asks the court to deny the request for disclosure of the information being sought.
6818 U.S.C. Section 2703(f).
69Evidence obtained through an unreasonable search or seizure (or through any other breach of the Charter) must be excluded in court if its admission would “bring the administration of justice into disrepute.” Canadian Charter of Rights and Freedoms, Section 24(2), http://laws.justice.gc.ca/en/charter/. At the same time, if admitting the evidence would not bring the administration of justice into disrepute, the evidence may be admitted even if it was obtained through an unreasonable search or seizure.
reasonable (1) if it is authorized by law, (2) if the law itself is reasonable, and (3) if the manner in which the search was carried out is reasonable. The Supreme Court of Canada has established three criteria for reasonable searches.\(^70\) First, although it might not be reasonable to insist on prior authorization in all circumstances, where feasible, prior authorization must be obtained before the search is conducted. Second, the person authorizing the search need not be a judge, but must act in a judicial capacity. Third, there must be reasonable and probable grounds to believe that an offense has been committed and that evidence of this is to be found at a particular place. These grounds must be established upon oath.

Subsequent cases have expanded these guidelines and have held that the standard of reasonableness is tied to the test of “reasonable expectation of privacy.” The “reasonable expectation of privacy” notion is not only relevant to determining whether a search was unreasonable, it is also central to determining whether the police conduct amounted to a search in the first place.\(^71\) As one justice of the Supreme Court of Canada held: “If the police activity invades a reasonable expectation of privacy, then the activity is a search.”\(^72\) To be reasonable, the expectation of privacy must be one that society is prepared to accept as reasonable. According to the Supreme Court, this involves assessing “the standards of privacy that persons can expect to enjoy in a free and democratic society.”\(^73\)


\(^{71}\)As one justice of the Supreme Court of Canada held in a case that considered the monitoring of an accused’s vehicle through an electronic tracking device: “It is clear that s. 8 of the Charter guarantees a broad and general right to be secure from unreasonable search where the person who is the object of the search has a reasonable expectation of privacy. In determining whether the beeper monitoring constitutes a search, the initial question is whether there is a reasonable expectation of privacy in respect of the monitored activity. If the police activity invades a reasonable expectation of privacy, then the activity is a search”: R. v. Wise, (1992), 70 C.C.C. (3d) 193 (S.C.C.).


\(^{73}\)The Supreme Court went on to say that: “This involves asking whether the persons whose privacy was intruded upon could legitimately claim that in the circumstances it should not have been open to the agents of the state to act as they did without prior judicial authorization”: R. v. Wong (1990), 60 C.C.C. (3d) 460 (S.C.C.), p. 478, paraphrasing the approach taken in a previous Supreme Court of Canada case, R. v. Duarte (1990), 63 C.C.C. (3d) 1 (S.C.C.).
In various high-tech searches, the Supreme Court has recommended a contextual approach that considers the following factors: (1) the nature of the information, (2) the place where the information was obtained, (3) the manner in which the information was obtained, (4) the seriousness of the crime, and (5) the nature of the relationship between the party releasing the information and the party claiming there has been a violation of his or her right to privacy.74

2. Statutory Standards for Search and Seizure

(i) General
The starting point for search warrants in Canadian criminal law is the traditional search warrant provision in the Criminal Code of Canada. Section 487 permits a justice of the peace to issue a warrant to searching a “building, receptacle or place.”75 Over the last decade, the Canadian Parliament has enacted several amendments to ensure that the Criminal Code adequately provides for warrants in the electronic environment.

In 1993, it amended the Criminal Code to provide for the issuance of warrants for electronic tracking devices76 and telephone number

---

74 In Computer Crime in Canada, Robert W.K. Davis and Scott Hutchinson expand upon these factors as follows: “(1) The nature of the information: is it highly personal information (for example, health billing record), information related to the operation of a purely commercial enterprise, or is it information that would not ordinarily be considered particularly private . . . ; (2) The nature of the relationship between the party that releases the information and the person now claiming that there has been a violation of his or her right to privacy: was the relationship commercial, professional, or personal, long-term or transient, compulsory or optional [and] does any sort of legislation promise privacy in relation to the information; (3) The place where the information was obtained: this seems to look at any sort of physical intrusion of a place in any sense related to the person asserting that there has been an unreasonable search associated with the information obtained; (4) The manner in which the information was obtained: was the information obtained by exercise of police authority on the third party custodian of the information, by some standing arrangement, with the consent of the third party custodian, or by positive action by the third party custodian; (5) The seriousness of the crime under investigation: is the offense a true crime, is it a real and pressing problem for the community, how heavily does society’s need for effective enforcement weigh in the constitutional scales.” Robert W.K. Davis and Scott C. Hutchinson, Computer Crime in Canada (Toronto: Carswell, 1997).


76 Criminal Code of Canada, Section 492.1. “Tracking device” is defined as “any device that, when installed in or on any thing, may be used to help ascertain, by electronic or other means, the location of any thing or person.”
recorders.77 The 1993 amendments also added a general warrant provision that permits the issuance of a warrant where no other provision in the Criminal Code or other statute authorizes the search.78 This section permits the issuance of a warrant authorizing a peace officer to “use any device or investigative technique or procedure or do any thing described in the warrant that would, if not authorized, constitute an unreasonable search or seizure in respect of a person or a person’s property.”79

Then, in 1997, Parliament amended the traditional warrant provision to provide for the execution of warrants in relation to data. The first addition expressly permits the search of a “computer system” and the copying of any data therein.80 The second requires those who exercise control over the building or place being searched to cooperate with the search and the copying of data.81

(ii) Authorization for Search Warrants

(a) Application on Oath

Search warrants are issued at the discretion of a justice upon the swearing of information by a law enforcement officer. The standards and procedures for issuing warrants are set out in the applicable provisions of the Criminal Code.82 Under Section 487, a justice may issue a warrant if he or she is satisfied that there are reasonable grounds to believe that:

- The item searched for is something in respect of which an offense has been or is suspected of having been committed;
The item will afford evidence of an offense or reveal the whereabouts of the person believed to have committed the offense;
- The item is intended to be used for the purpose of committing any offense against the person for which a person may be arrested without warrant; or
- The item is “offense-related property.”

As with other warrants, the issuance of a warrant under these provisions of the Criminal Code is discretionary; the Criminal Code does not say that, in such instances, a justice “must” issue a warrant; rather, it says that a justice “may.”

(b) Standard for Judicial Authorization

Depending on the type of warrant, the conditions that have to be met to satisfy the justice vary. To issue a warrant under the traditional warrant for search of a “building, receptacle, or thing” under Section 487, the justice must be satisfied that there are “reasonable grounds to believe” that the items searched for will be found in the building, receptacle, or place.

A warrant under Section 487.01 can authorize virtually any investigative technique. Because of the breadth of the powers that may be authorized under this section, the Criminal Code imposes a higher standard. To issue a Section 487.01 warrant, the justice must be satisfied that it is “in the best interest of the administration of justice” to do so (a prerequisite not required for other warrants) and that there is no other provision in the Criminal Code or any other federal law that would provide for a warrant, authorization, or order permitting the technique, procedure, device, or thing requested. In addition, the justice must be satisfied by information on oath that there are reasonable grounds to “believe” that an offense has been or will be committed and that information concerning the offense “will” be obtained through the use of the technique, procedure, device, or thing.

By comparison, to issue a warrant for an electronic tracking device or telephone number recorder, the justice need only be satisfied that there are reasonable grounds to “suspect” that an offense has been or

---

will be committed and that relevant evidence “can” or “could” be obtained. The difference no doubt corresponds to the degree of invasiveness of the search, the perceived expectation of privacy involved, and the different perceptions of the privacy interests that are at stake. These same factors are also the cornerstones of the constitutional analysis of unreasonable search and seizure under Section 8 of the Canadian Charter.

E. JURISDICTIONAL ISSUES

1. Whose Laws Apply in Transborder Searches?

Jurisdictional issues arise not only in determining which nation’s law applies to criminal conduct crossing international borders, but also in terms of what legal standards apply to searches and seizures transcending national borders (searches and seizures involving two or more nations). The nature of these issues and the approaches that have been taken are illustrated by two cases.

In the first case, the U.S. FBI was called in to investigate a series of intrusions “into the computer systems of businesses in the United States” that emanated from Russia. After contacting the Russian authorities several times seeking assistance without result, the FBI identified the Russian hackers and brought them to the United States under the guise of discussing a joint venture with an undercover security company named “Invita.” Upon arriving in the United States the two Russians, Alexey Ivanov and Vasily Gorshkov, offered to demonstrate their hacking skills by breaking into Invita’s own computers. To do so, Ivanov and Gorshkov sat down at Invita’s computers, allowed themselves to be watched as part of the demonstration, and logged on to their computer systems in Russia. They downloaded a scanning tool from the Russian system and used it to scan the entire network of computers located in the building where the small Invita office was located. The FBI recorded Ivanov’s and Gorshkov’s keystrokes through a computer program that generated a log of their activity.

During that “business meeting” and in other discussions, Ivanov and Gorshkov described the illegal hacking activity they conducted from Chelyabinsk, Russia, and claimed to have 15 to 20 people working with them. They admitted that they had hacked into a

85Brendan I. Koerner, “From Russia with LoPHT,” Legal Affairs, June 2002, at 35.
number of American businesses and obtained money from some of them. In that regard, Gorshkov said that they did not worry about the FBI “[b]ecause they can’t get us in Russia.” Unfortunately for them, however, the same did not hold true within the United States, and at the end of the meeting the FBI arrested Ivanov and Gorshkov and advised them of their rights. The Russian consulate was telephonically notified, and written notification was sent by fax to the Russian consulate the following day.

The FBI’s review of the keystroke logs showed that Gorshkov connected by telnet to a computer called “freebsd.tech.net.ru,” corresponding to his company’s website “tech.net.ru,” and that he had a username and a password. With this information the investigators determined that the site was still online, and they verified that the username and password provided access. They then contacted one of the prosecutors on the case to consider their next steps. Based upon a number of factors indicating that the evidence was at risk of being destroyed by the hackers’ associates in Russia, and in light of the previous lack of assistance from Russian authorities, the investigators downloaded evidence from the Russian computer, saved these data files to CDs, and sealed the CDs without looking at the content of the data files. The investigators reviewed systems files on the Russian computers only to the extent necessary to select relevant evidence. The government then applied to a U.S. magistrate judge for a warrant to search the data, which the court granted.

After being indicted for violating federal computer crime law, Gorshkov moved to suppress the evidence obtained from the Russian computers. The district court held (a) that the FBI’s actions did not violate the U.S. Constitution’s Fourth Amendment because the Fourth Amendment does not apply to searches and seizures on non-U.S. persons conducted outside the territorial boundaries of the United States; and (b) that Russian search and seizure law did not apply to the agents’ conduct in the United States. The District Court also

---

87 Id., Transcript, Government Exhibit 1B, at 122–23. With respect to Russian law enforcement, in one recorded conversation Gorshkov told undercover agents that when Russian authorities come after hackers the hackers either face time in jail, “or you’ll work for them.” Id., Transcript, Government Exhibit 1B, at 145.
88 Id., Transcript at 29; Transcript, Government Exhibit 9.
89 Id., Transcript at 106–11.
found that exigent circumstances had in fact existed, because “[t]he agents faced the impending likelihood that one of the Defendant’s co-conspirators in Russia would change passwords or pull the plug on the Russian computers.”91

The second case began when system administrators at the Rome Air Development Center (Rome Labs) at Griffiss Air Force Base in New York found a password “sniffer” on their network. The hackers had compromised Rome Labs’ systems and used them to attack other targets around the world. The Air Force’s Office of Special Investigations (AFOSI) identified one of the hackers as “Datastream Cowboy,” a citizen of the United Kingdom. AFOSI agents contacted New Scotland Yard, who had British Telecom monitor Datastream Cowboy’s (the hacker’s) telephone lines. Working together, AFOSI and New Scotland Yard developed probable cause and New Scotland Yard obtained a warrant to search Datastream Cowboy’s residence. They executed the warrant and seized incriminating evidence. Datastream Cowboy, also known as Richard Pryce, was prosecuted and eventually pled guilty to 12 counts of hacking.92

Both cases resulted in the apprehension and prosecution of the perpetrators, but they reveal two different modes of approaching the legal issues involved in transborder searches and seizures. The Gorshkov decision, if followed more widely, would leave cross-border searches and seizures subject to few legal standards: although the FBI examined the data pursuant to a search warrant, the court held that the Fourth Amendment to the U.S. Constitution did not apply to the U.S. agents’ extraterritorial access to computers in Russia or to their copying of data contained on the Russian computers, and that Russian law did not apply either. The Gorshkov agents proceeded unilaterally, after Russian authorities were contacted without result. This approach does not provide a sustainable basis for transborder searches and seizures because it would inevitably allow one state to transgress upon another state’s sovereignty by searching and seizing property belonging to that second state’s citizens, property that is physically located within that second state’s territory.

The agents in the Rome Labs investigation, on the other hand, operated on the basis of mutual cooperation and on the premise that the law governing a search and/or seizure is the law of the state where

91Gorshkov, 2001 WestLaw 1024026 at *4, n.2.
92See, for example, Richard Power, Tangled Web, Que Corporation (Macmillian, USA) 2000, at 66–67.
the property to be searched or seized is located. The American agents therefore contacted their counterparts in Britain and cooperated with the British officers, who, in turn, ensured that the evidence in possession of British citizens was collected in accordance with British law. One virtue of this approach is that it protects the rights of citizens by assuring them the protections established by their local law; another virtue is that it maintains comity by ensuring that law enforcement officers from one state do not unilaterally take action against property that is owned by a citizen of another state and that physically resides in that state.93

While informal cooperation proved effective in the Rome Labs investigation, that investigation only required the cooperation of officers from two culturally compatible nations; informal cooperation can be a less reliable mechanism when multiple states with varying legal systems are involved. In an effort to resolve the uncertainties resulting from informal cooperation, the Council of Europe’s Convention on Cybercrime requires signatory nations to adopt legislation or do whatever else is required to ensure “international cooperation . . . to the widest extent possible for the purposes of investigations or proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form of a criminal offense.”94 The G-8 has recommended similar measures.95

2. Interplay between Federal Law and State (or Provincial) Law in a Federal System

In countries with a federal system, where each internal state or province has its own law and its own circumscribed sovereignty, transborder search issues can arise internally as well as externally. The federal

93See, for example, Henry H. Perritt, Jr., Jurisdiction in Cyberspace, 41 Villanova Law Review 1, 87 (1996) (“a foreign search by U.S. officers potentially offends the sovereignty of the foreign state in which it occurred, thus potentially subjecting the United States and its citizens to retaliation, and the officials performing the search and seizure to punishment by the foreign country”).
system will typically have jurisdiction to conduct searches and seizures throughout the nation’s entire territory, but the states or provinces will have jurisdiction to conduct such activity only within the geographical confines of their respective territories.96

System conflicts can arise in either of two ways: One is a conflict between state and federal law; federal law and federally derived interpretations of federal law will typically prevail over state or provincial law.97 The other source of conflict is inconsistency or lack of reciprocity between the laws of two or more states; this type of conflict is a source of some difficulty for officers engaged in investigating cybercrime in the United States.98

F. BEST PRACTICES FOR CONSIDERATION OF LEGAL CONCERNS FOR INTERNATIONAL SEARCHES

1. What Are the Questions the Investigator Should Be Asking?

The first thing an investigator should determine is what formal and informal devices are available to search for and/or seize evidence located in another country. As the Rome Labs investigation illustrates,
informal methods of cooperation can be very effective, and they are usually the most expeditious means of obtaining evidence.99 The formal devices include “requests under mutual legal assistance treaties (MLATs), Letters Rogatory in the absence of a treaty or executive agreement, and subpoenas directed to U.S. citizens and permanent residents of the United States located abroad.”100

The investigator should therefore identify the country from which evidence is to be sought and determine whether a mutual legal assistance treaty encompassing the evidence exists between the United States and that country.101 The procedure for obtaining assistance under an MLAT is “generally faster and more reliable” than the older process of using a letter rogatory.102 If an MLAT is in force that applies to the type of evidence being sought, the investigator should prepare a request for assistance pursuant to the treaty.103 If no treaty is in force,

---

99See, for example, U.S. Department of Justice, U.S. Attorneys Manual—Criminal Resource Manual, Section 270, http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/crm00270.htm. (“Some tasks may best be accomplished by informal means while others can only be done by a formal approach.”) The most common informal methods are “police-to-police requests (often accomplished through United States law enforcement agents stationed at our embassies abroad)” and requests made “through Interpol for evidence (or . . . information) that can be obtained by foreign police without an official request.” This section of the Criminal Resource Manual also lists other informal methods.


101See, for example, U.S. Department of Justice, U.S. Attorneys Manual—Criminal Resource Manual, Section 268, http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/crm00268.htm. The investigator will have to demonstrate that evidence is located in that country (“foreign cooperation depends on the existence of articulable facts indicating that evidence is located in a particular jurisdiction.”).

102See U.S. Department of Justice, U.S. Attorneys Manual—Criminal Resource Manual, Section 276, http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/crm00276.htm (“The MLAT will define the obligation to provide assistance, the scope of assistance, and the contents of the request.”) MLATs are not “the only treaties that provide for legal assistance: some extradition treaties and many tax treaties contain such provisions.”

the investigator may have to rely on the more time-consuming Letters Rogatory procedure.\textsuperscript{104}

Another critical issue is determining whether the evidence being sought pertains to conduct that is illegal in the country whose assistance is being requested. Some countries grant assistance only if the conduct is illegal under their own law.\textsuperscript{105}

2. What Are the Sources for Guidance?

The U.S. Department of State website (a) offers general information as to how one goes about obtaining evidence from abroad, including advice on preparing Letters Rogatory; (b) lists the MLATs and executive agreements currently in force; and (c) provides specific information as to what is required in a series of different countries.\textsuperscript{106}

\begin{flushleft}


[D]ual criminality . . . is often required (for example, U.S./Netherlands MLAT). . . . [A] country can refuse a request if the request 'relates to conduct in respect of which powers of search and seizure would not be exercisable in the territory of the Requested Party in similar circumstances' (for example, U.S./U.K. MLAT). [S]ome MLATs . . . permit assistance only if dual criminality exists and if the offense is extraditable. . . . Therefore, if one country does not criminalize computer misuse . . . extradition may be prohibited.

Some countries also exclude assistance for specific offenses or specific types of cases (such as tax prosecutions) and some “limit assistance to the purpose stated in the request,” which means the evidence cannot be used for another purpose without obtaining the express permission of the country that provided it. See U.S. Department of Justice, \textit{U.S. Attorneys Manual—Criminal Resource Manual}, Section 269, cited above.

\end{flushleft}
The National Institute of Justice’s International Center maintains a website that provides links to the police and/or justice agencies of a number of countries.\textsuperscript{107} Interpol provides links to police-justice websites for most, if not all, of its 178 member countries.\textsuperscript{108} It is also possible to find such information directly on the Internet.\textsuperscript{109}

Interpol is a source of both information and assistance; it provides “an international framework for police forces to exchange information, share intelligence, and cooperate at an operational level.” Under its early warning system, Interpol maintains a list of Central Reference Points for participating police forces; officers can use a standard message form to seek assistance in investigating a cybercrime. Interpol’s contact information appears on its website.\textsuperscript{110}

The G-8 has established a high-tech points-of-reference initiative that is intended to supplement existing lines of communication between police agencies. Under the initiative, the participating nations nominate “a point of reference to be the first point of contact when a foreign police force needs urgent assistance in a case that involves electronic evidence. The points of reference are staffed 24 hours a day, seven days a week.”\textsuperscript{111}

The U.S. Department of Justice’s Office of International Affairs, which is part of the Criminal Division, “supports . . . state and local prosecutors regarding questions of foreign and international law,


\textsuperscript{110}See Interpol, Information Technology Crime—Regional Working Parties, http://www.interpol.int/public/TechnologyCrime/WorkingParties/Default.asp (early warning system consists of “an international 24-hour response system, National Central Reference Points (listing responsible experts within each of the 61 countries currently listed . . . and a formatted Computer Crime message format (to ensure that all the essential information is transmitted)”). Contact information is at http://www.interpol.int/Public/contact.asp.

including issues relating to ... mutual legal assistance treaties.”\textsuperscript{112} In addition, the Department of Justice’s Computer Crime and Intellectual Property Section may be able to provide assistance.\textsuperscript{113}

\textbf{V. Conclusion}

Law enforcement officials will increasingly be collecting electronic evidence, not only in cybercrime cases but also in investigations of other kinds of crime. This will require attention to both the practical and legal issues involved in accessing communications and stored data. Developing nations seeking to update their criminal laws for the digital age should simultaneously address the procedural standards for government access to communications and computer data, while balancing the protection of public safety with protection of privacy and civil liberties. They will also need to ensure that their investigators are adequately trained in the practical considerations surrounding the acquisition and analysis of digital evidence. The emerging body of international experience discussed in this chapter should provide suitable models for both the legal and practical aspects of the search and seizure of digital evidence.

\begin{footnotesize}
\begin{enumerate}
\end{enumerate}
\end{footnotesize}
CHAPTER 5

Public/Private Cooperation

I. Introduction

Cybercrime can take on many different forms. A company can be hacked, have its website defaced, be the victim of a distributed denial of service (DDOS) attack, have its proprietary or customer data stolen, have the confidentiality of private employee or customer data compromised, or be plagued by viruses. Individuals’ systems are also vulnerable; a home user’s computer and sensitive personal information can be accessed without authorization, or the computer can unknowingly be used to launch attacks. These crimes can be committed by disgruntled employees from within an organization, former employees, domestic and foreign competitors, hackers and “script kiddies,” 1 terrorists, and other nation states. At what point these attacks become criminal is dependent upon both local law and the extent of the damage inflicted. Whether and how a company responds to these attacks often involve a delicate evaluative balance among the potential financial loss or damage caused, the risks (legal, regulatory, and to business reputation) involved in reporting such attacks, and potential lawsuits and/or third-party liability, depending on the type of attack.

Public/private cooperation on cyber attacks and cyber criminal activities is important. When private and public sectors share and coordinate information relating to such crimes, they can each better

---

1The term “script kiddies” is used when referring to teenagers or young people who attack systems using tools developed and provided by others (hence, they use predeveloped “scripts”). They often use these tools to hack into systems or send viruses for ego gratification or peer acceptance.
understand how to respond and mitigate their impact. Information sharing, however, can mean different things to different people. For some, it is a way to develop or enhance information security ideas cooperatively; collaborate on joint responses; or share resources for detecting, preventing, and responding to security breaches and criminal activities. For others, it can mean divulging sensitive information or proprietary data, essentially giving the government, and potentially competitors, the “keys to the castle.” Some security researchers and professionals believe that information about security vulnerabilities, whether in networks or in host computers, should be shared not merely with industry or with government, but with academia and the general public as well. The security of networks and computers is part of the academic discipline of computer science, and the lack of security of networks and host computers is an important issue for everyone who uses the Internet.

Neither government nor the private sector can address these problems standing alone. Governments cannot solve the complex and multilayered problem of cyber security and critical infrastructure protection without the assistance of private organizations. The government needs a cooperative relationship with the private sector because, in most instances, the government does not own, control, or operate the networks that underpin the most critical sectors. The private sector needs the government because, no matter how large the corporation, it cannot by itself defend against attacks from terrorists or economic espionage by nation states.

A. BACKGROUND

The new millennium began in the midst of an unprecedented global economic boom, the foundation of which is the Internet and the productivity gains and efficiencies derived from rapidly advancing digital technologies that comprise the “information revolution.” This revolution, coupled with the fast-changing nature of information technology, has forever changed the way organizations do business.

These changes give new meaning to the adage that “information is power.” Whether the focus is the public or private sector, information about customers and competitors is invaluable. It can be used to predict customer demand, develop and market new products and services, and improve efficiencies in business operations. However, for those with malevolent or sometimes just mischievous intent, the bits and bytes of data flowing across this open-access, interconnected global marketplace can be used as a tool for fraud, deception, destruction, theft, and other malicious activities. Most data accessible on the Internet
is maintained by private companies. As such, this information—and their own internal databases—represent valuable corporate assets. Therefore, companies need to work together to maintain data and network security and assist law enforcement in combating cybercrime.

All people rely on critical infrastructures: electric power grids, railroads and airlines, oil and gas, banking and financial systems, and communications networks. Each of these infrastructures is dependent upon information technology and the global, interconnected network.

The rapid growth of connectivity has created new information vulnerabilities that can undermine economic growth or cripple critical infrastructures. Security of information, systems that process it, and their networks pose serious challenges for the people who manage them. Nowhere has the impact of these vulnerabilities been greater than in the ranks of law enforcement. Investigators in every agency and jurisdiction are confronted daily with new investigative and evidentiary issues that demand a high level of technical knowledge and skill. And, for the most part, they lack the resources, and sometimes the technical expertise, to effectively meet these challenges.

There are obviously varying degrees of threats within cyberspace ranging from the teenage hacker to the professional criminal. Hacking and virus incidents have the potential to be economically disruptive or even a threat to national security. Some attacks have already been very disruptive and costly to private organizations and individuals, disrupting their ability to transact business or simply use the Internet for a period of time. These relatively short-lived attacks have exposed to the world the underlying vulnerabilities of computer-dependent infrastructures to both lone hackers and coordinated attacks by sophisticated cyber terrorists who mean to cause harm.

The key problem is that while cyberspace has become the backbone of our highly integrated, modern e-commerce economy, it is also the underpinning of our defense and intelligence systems, as well as our nation's most critical infrastructures, such as communications, transportation, energy, and financial services. Cyber security has become everyone's responsibility, from the individual's personal computer to the large corporate and government computer networks. The U.S. government released in September 2002 a draft National Strategy to Secure Cyberspace, which provides a practical starting point for cyber security policy and guidelines.2

---

This chapter focuses on cooperation between private organizations and government agencies concerning information and infrastructure security and cybercrime. It adopts the fundamental premise that the sharing of information between the public and private sectors is necessary for the effective prevention and prosecution of cybercrime. Information sharing can help prevent and mitigate further cyber attacks, assist law enforcement in prosecuting criminal actions, and facilitate activities that foster better security practices for all information and communication technology (ICT) users. Part II provides an overview of types of cooperation; Part III discusses priority critical infrastructure sectors; and Part IV contains an analysis of benefits, costs, and legal bases for this cooperation. Part V looks at the components needed for cyber security cooperation, such as security standards, audits, insurance, and incentives; and Part VI concludes with an examination of international efforts to stimulate private and public sector cooperation.

II. Preliminary Issues

A. REVIEW INFRASTRUCTURE

In any effort to assess the role of public/private sector interaction and cooperation, a review of the subject country’s governmental, political, and economic infrastructure is essential. This involves identifying the essential organizations within government, political leadership, and business, without which these sectors could not function. The particular aspects of each of these areas will determine the strengths, vulnerabilities, and issues that need to be addressed and factored into the equation in developing a strategy for dealing with cybercrime.

In developed and developing countries alike, industries and governments that are highly networked or dependent on information technology are inherently vulnerable to cybercrime. These systems can comprise the critical infrastructure on which a nation’s economy and security depend. Consequently, governments and private sector industries that own infrastructure each have an interest in initiatives that detect and deter cybercrime, particularly because it inhibits growth. In developing countries, this interest is even more fundamental because cybercrime adds insecurity to the overall business environment and deters foreign direct investment (FDI), restricts the benefits of adapting new technologies, and inhibits economic growth.

B. PRIORITIZE CRITICAL SECTORS

In developed countries, government and industry have implemented policies and mechanisms for the exchange of information concerning
cybercrime threats and defenses. These initiatives seek to combine the public and private sectors’ respective strengths on a foundation of mutual trust. While law enforcement may have investigatory expertise and intelligence that cuts across business sectors, industry will generally have a keener understanding of its business needs and its particular system’s strengths and vulnerabilities. Many organizations also benefit from global programs designed to facilitate international public/private partnerships and protect critical infrastructure.

The United States has addressed information exchange by means of several mechanisms. Pursuant to Presidential Decision Directive 63 (PDD-63), May 22, 1998, federal government agencies were designated as lead agencies for eight infrastructure sectors. These infrastructure sectors included in the U.S. “critical information infrastructure” and their respective designated lead agencies are:

- Communications: Department of Commerce
- Electrical power and gas and oil systems: Department of Energy
- Banking and finance: Department of the Treasury
- Transportation: Department of Transportation
- Water supply systems: Environmental Protection Agency
- Public health services: Department of Health and Human Services
- Emergency fire services: Federal Emergency Management Agency
- Emergency law enforcement services: Department of Justice/FBI

In addition, PDD-63 established two other organizations:

- The Critical Infrastructure Assurance Office (CIAO), which was established to coordinate the work of the sector lead agencies and to affect outreach to private industry across all infrastructure sectors.
- The National Infrastructure Protection Center (NIPC), which was created within the FBI to coordinate information concerning cyber attacks, and, if criminal in nature, to work with law enforcement agencies at all levels to prosecute. The NIPC has

---

3The text of Presidential Decision Directive 63 can be found at http://www.ciao.gov/resource/paper598.html. Presidential Decision Directives are formal policy positions of the President and, as such, government agencies and departments are expected to comply with them.

4For additional information on the Critical Infrastructure Assurance Office and links to useful resources, see http://www.ciao.gov.
also established an industry outreach effort called InfraGard, with chapters existing at more than 60 FBI field offices across the United States. InfraGard works closely with private sector companies to help them prevent and respond effectively to cyber criminal activities.\textsuperscript{5}

Industry sectors were also encouraged to form Information Sharing and Analysis Centers (ISACs) to exchange real-time operational information, anonymously, about cyber attacks and suggested ways to overcome them.

More recently, Executive Order 13231, issued October 16, 2001,\textsuperscript{6} established the President’s Critical Infrastructure Protection Board. The board has several standing committees that address various aspects of information infrastructure assurance. The Private Sector and State and Local Government Outreach Committee, chaired by a senior official of the U.S. Department of Commerce, focuses on encouraging public and private cooperation. However, many of the other standing committees also have a private sector aspect.

The United States is not alone in needing to face these issues. All countries, developed or developing, need to understand the relationship among ICTs, security, and economic well-being. In developed economies, businesses have become dependent on the information technology that runs everyday operations and links companies with networks of suppliers, retailers, and the public worldwide. The foundation of developed economies today is technology; the security of these information systems is, therefore, fundamental to the economic health of a country.

In many developing economies, much of the ICTs utilized are still not widely deployed, or even available. Overcoming the “digital divide” is one of the goals of the UN, World Bank, G-8, and many other international development organizations. In order to realize the potential economic and social benefits of ICTs, one of the key issues for developing countries is to have an environment that encourages electronic commerce while not providing a convenient place from

\textsuperscript{5}For additional information on the National Infrastructure Protection Center and InfraGard and links to useful resources, see http://www.nipc.gov and http://www.infragard.net, respectively.

\textsuperscript{6}The text of Executive Order 13231 can be found at http://www.ciao.gov/News/EOonCriticalInfrastrutureProtection101601.html. Executive Orders are formal orders from the President of the United States that have the force of law.
which computer criminals can attack computer systems or be afforded protection from cybercrime prosecution. An adequate legal framework and effective public/private cooperation designed to create a secure operating environment are critical factors for effective use of ICT in economic development.

When seeking to improve cyber security, countries might find it helpful to prioritize the industry sectors most vulnerable to cybercrime and most crucial for security. In developing countries, many of the critical infrastructures are state-owned enterprises. Even so, they service private sector entities in the country and public/private sector cooperation is as vital as in areas that have been privatized. Indeed, industry/government partnerships facilitate the exchange of security information, monitoring of systems, and effective responses to cyber attacks that benefit government and industry alike. Because of the economic dimension of security, cyber security policies should encourage private sector actors to balance security and business needs and should incorporate business people in the policy process. Business leaders can aid in identifying issues and potential solutions that are practical and not overly broad. Nongovernmental organizations (NGOs) can play a useful role in organizing private sector interests and facilitating organized communication and interaction with the public sector on ICT security issues and the development of the legal/regulatory framework.

Although any business using information technology or networked with other parties is susceptible to cybercrime, certain sectors are especially vulnerable. In developed countries, these types of industries have been at the forefront in public/private cooperative efforts against cybercrime. Developing countries may wish to prioritize cyber security policies directed toward these sectors, listed in no particular order. How a country chooses to prioritize may depend on its unique circumstances and the development of its infrastructure.

1. Information Technology Industry

Information technology companies, including Internet service providers (ISPs), Internet backbone providers, application service providers (ASPs), website hosting companies, and e-commerce companies are frequent victims of cybercrime. Assaults, including hacking, viruses, worms, denial-of-service attacks, and economic espionage, limit these companies—and their countries—from realizing the social and economic potential of the Internet. Also, the ability of the Internet
to serve as a backup communications system during emergencies underscores the need for effective cyber security measures.

2. **Communications**

Like Internet service providers, telecommunications carriers are highly networked and make extensive use of information technology. The importance of a nation’s communications systems necessitates policies for preventing cybercrime and preserving service in case of an attack, especially for crucial government officials and emergency response crews.

3. **Financial Services and Banking**

Fraud is one of the most frequently perpetrated types of cybercrime and inhibits a country’s ability to attract foreign direct investment. Technology improves the efficiency of financial services and lowers transaction costs but also exposes businesses to outside security threats. Governments should also take specific steps to stem the use of their banking systems for money laundering.

4. **Chemical, Biological, and Nuclear Security**

The pernicious use of information technology to cause a severe environmental or public health hazard is an emerging threat. Governments should ensure the proper protection of systems controlling chemical plants, nuclear facilities, laboratories, and other institutions handling potentially dangerous materials and the security of systems that manage vital natural resources.

5. **Utilities and Transportation**

Information technology helps improve the reliability of utility and transportation systems, but it also introduces vulnerabilities. A sophisticated cyber attack could take down energy grids, air traffic control systems, rail systems, airline systems, or traffic management systems.

6. **Government Information Systems**

Government agencies maintain databases and have a responsibility to citizens to securely manage the data stored in them. Attacks on government systems damage the credibility of governments and diminish the confidence of citizens that is vital to effective governance. National, regional, and local government systems are equally susceptible to attacks similar to those described elsewhere.
7. Ordinary Computer Users and Businesses

Any computer user or business with a personal computer that interacts with other computers is susceptible to viruses, hacking, and other cyber crimes. Governments may wish to educate businesspeople about cybercrime and help them prevent avoidable cyber attacks through dissemination of best practice materials and guidance. This public/private interaction is an excellent starting point for building the trust necessary for effective industry/government information sharing. ISPs may wish to warn their customers about vulnerabilities and educate them about tools and practices for safeguarding their home computers. As discussed in greater detail in Chapters Three and Four, police forces should be trained on how to preserve cybercrime evidence and assist victimized businesses.

III. Analysis

A. INFRASTRUCTURE MANAGEMENT

1. Overview

Structural efficiencies and benefits will result from an established and credible information sharing arrangement between private organizations and government agencies of data and information concerning electronic security and cybercrime. To create and maintain such a collaborative arrangement, existing and planned critical infrastructures must be periodically assessed and evaluated, including how they are managed. A review of the subject country’s information infrastructures should also be performed to determine the strengths, vulnerabilities, and issues that may need to be considered in developing an effective strategy for dealing with cybercrime. This review and analysis is similar to the review of the subject country’s governmental, political, and economic infrastructure mentioned in Part II above.

In this regard, the subject country’s regulatory mindset and legal framework can have a significant impact. Thus, in examining the critical infrastructure, it is important that the role and restrictiveness of the applicable laws and regulations be considered, as well as the culture of the regulatory agencies or ministries that oversee those laws/regulations. Given the private sector’s desire for autonomy, particularly in those countries that tend toward a more liberal approach in regulating private industry or sectors, a delicate balance must be struck between emphasizing the incentives in garnering the private sector’s cooperation in information sharing initiatives in return for incurring potentially greater risk and exposure to law enforcement.
and liability concerns. Governments must keep in mind, however, that the private sector includes individual users who arguably have a right to know about security vulnerabilities so that they can make informed choices about their own Internet use. At all times, governmental decision-makers must work closely to ensure that the subject country’s policies recognize the clear benefits to be derived by having strong defensive and offensive measures in place to combat cybercrime: security for both domestic and foreign investment and encouragement of technological innovation and robust economic growth—both realized and potential.

2. National/Regional/Local Issues

In addressing a subject country’s infrastructure, one other area that requires examination includes the differences that may exist between national and regional authorities (in the U.S., this would be the federal, state, and local authorities). In order to avoid conflict and duplication of efforts, a clear delineation of the separate and overlapping roles of each authority should be made. This will often require additional coordination among national, regional, and local authorities, and should include an open dialogue regarding the separation of powers and responsibilities of the relevant authorities. As always, it is also important to involve the private sector at each of these levels of government, because there is a shared public/private sector responsibility for information and infrastructure security.

B. INFORMATION SHARING AND ANALYSIS CENTERS (ISACs)

Probably the best examples of public/private sector information sharing are the Information Sharing and Analysis Centers (ISACs), which have been voluntarily formed by private members within specific industries, under the premise that sharing information among industry specific groups can help fight cyber threats. ISACs have been cited around the world as models for cooperation and information sharing between and among the private and public sectors.

For further information, see the websites for the following ISACs: chemicals industry (http://www.chemtrec.com/); electricity sector (http://www.nerc.com/~filez/cip.html); emergency fire services (http://www.usfa.fema.gov/dhtml/media/02-nipc.cfm); emergency law enforcement (http://www.nipc.gov/infosharing/infosharing5.htm); energy (http://energyisac.com/); financial services (http://www.fsisac.com/); food industry (http://www.fmi.org/isac); information technology (http://www.it-isac.org/); surface transportation (http://www.surfacetransportationisac.org/); telecommunications (http://www.ncs.gov/nec/main.html); water (http://www.waterisac.org/); and worldwide (http://www.wwisac.com).
Depending on the ISAC, members have a lot of leeway in deciding how much information (including their identity) they will review. The information shared can be either anonymous or attributable at the discretion of the member. The identity of members may be either secret or public. Government entities may sometimes, but not always, participate directly in the information sharing functions of an ISAC. A comparison between two different models would include the Financial Services ISAC (FS-ISAC) and the National Communications System’s National Coordinating Center, which functions as the Telecommunications ISAC (Telecom-ISAC). The FS-ISAC consists solely of private sector members who remain confidential and prefer to use anonymous reporting. Because no government agency has direct access to FS-ISAC data, laws such as the Freedom of Information Act (FOIA) or those allowing public access to government information do not apply. In comparison, the Telecom-ISAC builds upon historical government/industry coordination, and members include both government and industry entities, but they still maintain confidentiality of incident reporting. Since ISACs are independent, each sector center decides how to best organize for optimum results. For example, the Information Technology ISAC states on its web page:

The IT-ISAC is a not-for-profit corporation serving the information technology industry and established to report and exchange information concerning electronic incidents, threats, attacks, vulnerabilities, solutions and countermeasures, best security practices and other protective measures. The organization will collect, synthesize, and disseminate information about threats and coordinate the information technology industry’s response to such threats. An example of a current cooperative public/private information sharing venture is InfraGard, a joint effort between private industry and the National Infrastructure Protection Center (NIPC). Its function and goals as set forth on its website are:

InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a cooperative

---

9 See http://www.it-isac.org/.
undertaking between the U.S. Government (led by the FBI and the NIPC) and an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to increasing the security of United States critical infrastructures. The goal of InfraGard is to enable the flow of information so that the owners and operators of infrastructure assets can better protect themselves and so that the United States government can better discharge its law enforcement and national security responsibilities.\footnote{For more detailed information, see the InfraGard website at http://www.infragard.net.}

InfraGard meetings, often held quarterly in over 60 chapters/cities in the U.S., typically are open only to members (companies and organizations) that have agreed to a common code of ethics. The meetings provide a forum for the informal exchange of information between the private sector and government agencies as well as an opportunity to meet and discuss vulnerabilities and cyber threats. InfraGard also provides members a means of sharing sensitive information with other members and the government subject to a signed confidentiality agreement.

C. BENEFITS OF INFORMATION SHARING

The common benefits that accrue to ISAC members are:

- Early notification
- Relevant information
- Industry-wide vigilance
- Subject matter expertise
- Trending, metrics, and benchmark data

A recent GAO Report entitled \textit{Information Sharing: Practices That Can Benefit Critical Infrastructure Protection}, provides a good analysis of some of the hurdles facing public/private information sharing and suggests factors necessary for effective information sharing including:

- Establishing trust through personal relationships.
- Creating secure communication mechanisms (regular meetings and secure websites).
- Developing standards and agreements that ensure that shared information is secure (may need legislative changes).
Recruiting and developing personnel with the necessary talent.  
Obtaining the support of senior levels in both government and industry.  
Obtaining and maintaining adequate funding.  

The “free rider” issue, however, comes into play with information sharing programs. If some companies share information, then the damages caused by the criminals and the resulting damage can be prevented without every company’s cooperation. Therefore, the incentive for sharing information is reduced and the “free rider” issue becomes a problem; companies hold back on sharing information with the attitude that another company will share and provide the means for addressing the problem. Businesses must be convinced that their participation is important in order to identify trends and vulnerabilities, and they must be convinced that there will be more economic benefit from their participation in the information sharing process than the cost of belonging to the ISAC.  

The greatest potential benefit of information sharing among the public and private sectors is the pooling of resources to combat destructive, costly, and challenging electronic crimes. An example of such collaboration is the recent effort by companies and organizations (mostly through their ICT networks) to share virus alerts and patches and establish cooperative response teams to rapidly respond and mitigate the impacts of the NIMDA worm (2001) and the Code Red virus (2001). Probably the best reason for companies and government to share information to combat cybercrime is that the cyber criminals are very experienced at information sharing and will have the upper hand if industry and government do not band together. The Internet is full of websites on which hackers, script kiddies, and virus authors share the results of their exploits, disclose new vulnerabilities they have uncovered, and give instructions for coordinated computer attacks and breaking into systems. Virus Exchanges and Conferences (such as DefCon) also foster and encourage the sharing of information within the hackers’ network.  

Information sharing also helps organizations better understand the costs associated with cyber crimes, and it can help businesses measure the cost/benefit of participating in cooperative public/private sector

---


12DefCon is an annual hacker’s conference. See http://www.defcon.org/.
exchanges. The annual Computer Security Institute CSI/FBI Computer Crime and Security Survey of 2002 helps provide some perspective. Though most of the over 500 organizations polled provided information anonymously, the aggregate 1997 to 2001 losses to responding businesses from theft of proprietary information, financial fraud, viruses, and system penetration were around US$1.5 billion.¹³ Ninety percent of the companies reported losses from computer intrusions. Although fewer than half of the respondents could quantify the corresponding losses, it is clear that the costs of cybercrime continue to grow every year. For the fifth year in a row, more respondents (74%) cited their Internet connection as a more frequent point of attack than their internal systems (33%).¹⁴ Only 34% of respondents reported the intrusions to law enforcement, down from 36% in 2001, but up from 16% in 1996.¹⁵

The number of successful cases prosecuted compared to the extent of illegal activity is small. To a certain extent, law enforcement authorities must overcome a reputation for being understaffed and unable to respond to “everyday” reports of cybercrime activities. The benefit businesses receive from information sharing would increase if the mechanism for reporting and sharing information were more effective and responsive.

D. POTENTIAL RISKS OF INFORMATION SHARING

A private organization’s decision to share information regarding cyber crimes with the government will depend on a number of factors. Private organizations should consider and balance the following:

1. Disclosure of Proprietary or Sensitive Information

An important business concern arises from a fear that by sharing information, a company may be allowing its competitors access to competitively sensitive or proprietary information. Although many ISACs operate under an agreement that all submitted information will be “sanitized,” or stripped of all identifying information, in small industry sectors it is not difficult to figure out who had a problem and

---

¹⁴2002 CSI/FBI Report at 8.
¹⁵2002 CSI/FBI Report at 20.
exploit that information. There is the additional concern that if information is shared with the government, it will not be adequately protected or could be inadvertently released or made public through Freedom of Information laws. In order to encourage an exchange of information between the public and private sectors (especially with regard to reporting cybercrime activity and allowing government access to sensitive data), these concerns regarding protecting information must be addressed. Of course, to the extent a company has already been victimized by a hacker, it already may have lost its sensitive data, thus, reporting the cybercrime could result in enhanced protection.

2. Risks to the Organization’s Reputation and Stock Price

Both insiders and outsiders can attack networks. When an insider is responsible for an attack or cybercrime, the reputation of the organization for effective management will especially suffer when these instances are made public. Even when a company is a victim of an external attack, previous studies have shown that this can result in a lack of confidence in the company and even a drop in the company stock price. Consequently, many companies do not report cyber security incidents. There is the risk, however, that by not reporting security compromises, a company may endanger its relationship with its customers, especially if attackers gain access to sensitive customer information or use the company’s computers as a platform to attack other systems.

3. Reallocation of Resources

Information security can be costly. The mechanisms for information sharing and management and professional staff time are costs that must be borne by the organization. To the extent that resources are allocated to information sharing, it reduces the resources that can be used for implementation of other aspects of security. To date, the financial feasibility of ISACs is uncertain.

4. Disruption of Business Operations

Another reason companies are loathe to report cyberincidents is the fear that law enforcement might disrupt their business operations.

---

through its investigation. An investigation of a cybercrime or other computer attack may result in both hardware and staff being “offline” and unavailable to service a business’s regular operations for a period of time. For example, during an investigation, an organization’s servers and computers may be seized or quarantined in order to preserve evidence for trial. Imaging the desired data by law enforcement is one approach that is proving useful in minimizing any disruption. Routine coordination between a company’s systems administrator and security manager and law enforcement representatives before any cybercrime or computer attack occurs also helps minimize interruptions to business operations. This cooperation can result in a protocol that would both serve as a checklist for the company and provide essential information for law enforcement authorities, minimizing the potential for damage when an attack occurs and significantly reducing the time or scope of disruption.

5. Liability

There is a legitimate legal basis to believe that courts could hold a person or corporation liable for inadequately securing its data and network. Entities that allow their networks to be penetrated, infected with viruses, used as launching pads for denial-of-service attacks, or who allow their data to be sabotaged or stolen could wind up involved in lawsuits from shareholders, business partners and customers, and third-party victims. Recognizing that negligence is a key principle of liability, if Boards of Directors, officers, network operators, and information systems managers do not take the precautions a reasonably prudent person in the same situation would have, then they may potentially be held responsible for the criminal or civil wrong of another.

There are real liability risks associated with security breaches. When sharing information, these risks may increase. Potential liabilities include:

- Liability for improperly disclosing personal customer information under statutory or contractual protections.
- Shareholder derivative suits for improper management related to network and data security.

Liability for insufficient security measures under statutes or regulations.

Tort liability for unreasonably insecure networks that result in injury to others, individuals or businesses, including third-party liability to customers and business partners.

Damages from these liabilities may, in part, be managed through insurance.

E. LAWS THAT IMPEDE INFORMATION SHARING

In order for there to be an effective exchange of useful information between the public and private sectors, several legal/regulatory concerns must be addressed.

1. Antitrust

The first set of concerns revolves around restrictions on the sharing of certain information between competitors. Generally referred to as antitrust or anti-competition laws, industries are restricted in their ability to collaborate with their peers in joint information reporting and sharing, and there are differences between industries. Without specific statutory or regulatory grants of immunity, some industries can only share aggregate data that do not disclose marketing data, pricing, or strategy. These types of restrictions are considered beneficial in terms of consumer protection and avoiding monopolistic practices by the private sector, but they can also hinder the sharing of information that could assist in spotting cybercrime trends or vulnerabilities common to an industry. There are permitted exceptions, which allow sharing of information for reporting suspected fraudulent or criminal acts. However, these can also vary by both industry and regulatory body. Currently, in the United States, for example, in order to be certain that an industry’s information sharing activities were not in violation of antitrust laws, a representative would need to ask for a letter of exemption for this activity from the Department of Justice. In order to identify industry-wide concerns or trends regarding cyber crimes, a careful review of the antitrust restrictions should be undertaken in order to encourage companies to collaborate, share, and report information that could identify common vulnerabilities.

Efforts are currently under way, mostly by network systems administrators and information security personnel, to share information on known cyber attacks and system vulnerabilities. While these types of professionals collaborate in information sharing, broader involvement
by private industry’s senior management (including general counsels and legal departments) is only just now beginning to develop. Joint public/private sector initiatives already under way in the United States, such as InfraGard and the Information Sharing and Analysis Centers (discussed above) have received increasing interest and support in light of the terrorist attacks of September 11, 2001.

2. Freedom of Information Laws

The U.S. Freedom of Information Act (FOIA) laws mandate public access to large portions of government-held information. The goals of these laws are to provide transparency and accountability in government and the resultant benefits from government acting in the public light. There is often a tension between these goals and other societal goals, including privacy and security. With regard to businesses, FOIA provides exemptions to the disclosure of trade secrets or sensitive/proprietary business information and certain disclosures made to law enforcement. However, the lack of clarity about how the FOIA applies to the sharing of information security breaches and other cybercrime information may serve as a barrier to sharing of information. Legislation has been proposed in the United States that would create a specific exemption to public disclosure of this kind of information. There is considerable debate over whether such an exemption is good public policy or necessary given existing law. Critics argue that companies need to have incentives to improve security, and that restricting information about security vulnerabilities makes it harder to hold companies accountable for failing to fix known weaknesses. On the other hand, without FOIA protection for voluntarily submitted data, private industry is unlikely to provide

---

185 U.S.C. Section 552(b)(4)–(b)(7); the text of this provision can be found at http://www4.law.cornell.edu/uscode/5/552.html.
19Several laws currently pending in the U.S. Congress address this issue and would protect information shared with the government regarding information security. See Senate Bill 1456, Critical Infrastructure Information Security Act of 2001, http://www.senate.gov/~bennett/s1456.html, which would provide that information shared voluntarily under a new exception to the FOIA could not be used in civil litigation unless bad faith were shown, and could not be used for any other purpose without permission; Senate Bill 3188, Cyber Security Enhancement Act, is similar to House of Representatives Bill 2435, Cyber Security Information Act, which would protect voluntary disclosures and provide an antitrust exemption for such cooperation among companies. Several public-interest groups, including the Electronic Privacy Information Center, the Center for Democracy and Technology, and the Electronic Frontier Foundation, have criticized these bills as impeding accountability for security weaknesses.
security vulnerability information to the government in the first place and, therefore, the public still will not have FOIA access to it.

3. Data Privacy

Internationally, the European Union’s Data Protection Directive is at the forefront of data privacy initiatives. It requires, among other things, that appropriate security measures be adopted to protect the privacy of individually identifiable information, and mandates that sharing of information requires an individual’s consent. This could clearly create problematic situations regarding information sharing. Some countries, such as Australia, have an independent Federal Privacy Commissioner to implement laws; provide policy guidance on privacy issues in response to requests from federal and territory government agencies and the private sector; investigate complaints from individuals about interferences with privacy; publish guidelines, milestones, and audits; and assist with education about privacy issues.

In the U.S., several relatively new laws protect the privacy of personally identifiable information. The Gramm-Leach-Bliley Act (GLBA) protects customer financial information. Except as permitted by law, the GLBA requires that a financial institution give consumers notice and an opportunity to opt-out of the sharing of certain nonpublic information with unaffiliated third parties. In addition, GLBA requires financial institutions to implement both physical and electronic safeguards to protect such consumer information. The Health Insurance Portability and Accountability Act (HIPAA) mandates individual access to health information, protection of privacy, and the implementation of security measures to protect personal health information. To comply with HIPAA, draft regulations put forth by the Health & Human Services Department mandate privacy and security of medical and health information.

The USA PATRIOT Act of 2001 was signed into law on October 26, 2001. It changes the bank secrecy regulations, expands the FBI’s wiretapping and electronic surveillance authority (including computer conversations), imposes stronger penalties for harboring or financing terrorists, and increases the number of crimes considered terrorist acts. The USA PATRIOT Act permits the owners or operators of communications networks (which can include businesses, universities,
and other computer systems operators) to authorize law enforcement to intercept electronic communications or activity on the network, so long as the hacker is not a customer.

There are other legal authorities that may bear on information sharing, such as the Privacy Act (regulates government-stored information) and the Fair Credit Reporting Act (regulates information collected by credit agencies). Also in the United States, there are various consumer protection laws administered at the national level by the Federal Trade Commission and at the regional level by the states’ attorneys general. The interplay of all these various laws and the clear public policy mandate for privacy of certain information will need to be evaluated and addressed by both the public and private sectors in order to facilitate a cooperative sharing of cybercrime information.

Methods to reduce the costs to businesses include:

- Protection of the source of information that is shared.
- Clarification of duties of data protection that could conflict with the disclosure of information.
- Clarification of the antitrust laws.

It is possible these goals could be accomplished through legislation or administrative rules.

IV. Some Components of Cyber Security Cooperation

A. RISK MANAGEMENT APPROACHES

1. Software Industry Assistance and Customer Information Sharing

Security resources within companies are limited, and even large companies with large budgets find it difficult to meet the need for fighting cyber criminals and securing software, databases, and networks. In fact, security professionals express the view that, overall, the commercial sector is not adequately addressing the security issue. Many known vulnerabilities are not addressed in a timely fashion. In some cases, academic researchers and security professionals have informed software companies about vulnerabilities in their products to

---

22See The Privacy Act of 1974, 5 U.S.C. Section 552a, [link]
no avail; only the threat or actual public disclosure of weaknesses causes companies to take action. It is understandable that companies do not want the negative publicity that may accompany the disclosure of security holes, but this kind of secrecy may endanger a country’s collective effort to secure its networks and computers. The sharing of information regarding software vulnerabilities could benefit both the public and private sectors as a whole. When smaller or weaker entities with fewer resources are able to address security vulnerabilities through cooperative efforts, the entire system is strengthened.

Information sharing can be facilitated by public sector initiatives that (a) establish centers for sharing information on an anonymous basis or serve as an intermediary where the direct sharing of information among industry is difficult, (b) create a central alert point for technical information and assistance regarding security risks and fixes, and (c) organize a public/private group comprised of all stakeholders (industry, government, academia, NGOs) to begin a dialogue on ICT security risks and develop ways to work together.

2. Performance-Based Operating Guidelines

Performance-based operating guidelines set by industry or industry and government together are preferable to standards or a regulatory scheme mandated by government alone. Standards are generally set by independent standards-setting bodies, including many well-established organizations, such as the International Standards Organization (ISO), the American National Standards Institute (ANSI), and the International Engineering Task Force (IETF). However, nearly all of the independent standards-setting bodies in the U.S. work with the U.S. National Institute of Standards and Technology (NIST), an organization within the U.S. Department of Commerce. For more than a quarter century, NIST has worked to develop standards relating to security, including encryption, computers, communications equipment, and law enforcement. The public and private sectors can work together on common security problems to arrive at performance-based operating guidelines that will facilitate global cyber security.


One important approach to security standards is called the Common Criteria Recognition Arrangement (Common Criteria), which was developed in 1998 by NIST and similar organizations in a few other countries.

countries. The Common Criteria help define requirements for certain information security technologies, giving consumers a vehicle for expressing their requirements and a common framework within which consumers and producers can exchange views concerning what security features are needed and which are feasible. In 1999, the Common Criteria became effective as an international standard (ISO/IEC 15408). They now serve as the basis for a 14-nation formal arrangement that recognizes the results of security evaluations conducted in the participating nations. Using the Common Criteria, consumers and producers of information technology products and systems are now able to develop and implement well-defined sets of security requirements and specifications in many areas, including operating systems, database management systems, networks and telecommunications systems, smart cards, and other information-intensive applications.

Industry/government cooperation was essential in developing and updating the Common Criteria. Without this cooperation and consumer involvement in helping to shape the demand for evaluated products through the security requirements definition process, the overall goal of improving the security of information products and the confidence consumers have in these products would be more difficult to achieve. The latter goal is significant because greater confidence in the security features of individual component products will spur the development of more secure systems and networks for federal agencies and private sector enterprises, and lead to a more secure information infrastructure. The drawback to the Common Criteria, however, is that it imposes significant costs on security software developers to have their products tested and certified as meeting the Criteria, thus impeding innovation and security solutions when we need them most.

4. Security Audits and Management Oversight

Companies and governments alike need to conduct regular security audits of their ICT systems. External auditing focuses on specialized third-party service audits of information processing facilities, operations, and related management. These audits are an important element of the management of information and infrastructure security and are usually performed by experts who specialize in security vulnerability assessments and penetration testing at the direction of

\]

\[27\text{Audit and assessment standards include BS7799/ISO17799 and AICPA/CICA’s WebTrust, http://www.cpawebtrust.org/Security_fin.htm.}\]
the chief security officer, chief information officer, or internal auditor. Sometimes these experts interact with a company’s outside auditors regarding the availability, confidentiality, and integrity of corporate data.

As part of the “business case” approach to information security, it is important that senior management exercise oversight of the security of data and networks and how technology is being used. The Institute of Internal Auditors, American Institute of Certified Public Accountants (AICPA), the National Association of Corporate Directors, the Information Systems Audit Control Association (ISACA), and the Assurance Services Development Board of the Canadian Institute of Chartered Accountants (CICA) have done some important work in advancing ICT security and raising the awareness of senior management regarding these issues. 

A few of the issues of interest to executive management include (1) the potential for negative impacts on shareholder values, (2) insurance issues, both for the organization and for directors’ and officers’ liability, (3) liabilities arising from cyber attacks and privacy violations, and (4) compliance with regulations and laws. Because ICTs are an integral part of physical security, executive and personnel protection, and information and infrastructure security, board-level risk management committees should exercise oversight of the combined security risks, including ICT security, and interact with the board auditing committee to ensure compliance with applicable laws, regulations, contracts, and corporate policies.

5. Insurance

Insurance has historically played a significant role in motivating good business behavior. Increasingly, insurance companies are treating cyber security as a new area of risk management and coverage because most corporate general liability policies do not cover cyber incidents and resulting losses incurred. Network security insurance specialists seek to evaluate companies’ risks and design solutions combining risk management advice, technology, and insurance. According to one

---


insurance company’s experience, 85 percent of its client companies reported at least one computer security breach in 2000. Ninety percent reported vandalism attacks, 78 percent reported denial-of-service attacks, and 64 percent acknowledged financial losses due to these attacks. The average loss was US$2 million. In explaining the “business case” to company CEOs, insurance companies note that the traditional risks covered by insurance are changing, with a need now to focus on critical information risk management.

The risks insurance should cover include legal liability to others, security breaches resulting in loss of business continuity, data, and damage to the network, website integrity, damage to reputation, loss of market capitalization, and shareholder lawsuits. The private insurance sector plays a unique role in beneficially motivating companies’ behavior by adjusting the price and availability of insurance based upon security measures implemented by clients.

V. International Efforts to Stimulate Private and Public Sector Cooperation to Combat Cybercrime

Many international organizations recognize the need for private and public sector cooperation to secure information infrastructures and to combat cybercrime. As described below, such organizations are developing ways to facilitate partnerships that share information and experiences, best practices, management procedures, and technical solutions.

A. ACTIVITIES OF GOVERNMENTAL BODIES

1. European Union (EU)

The eEurope Action Plan policy initiative was initially adopted in June 2000 by the Feira European Council.30 The policy provides for the establishment of an EU Forum for law enforcement agencies, Internet service providers, telecommunications operators, civil liberties organizations, consumer representatives, and data protection authorities to raise public awareness of the risks posed by criminals, promote best practices for security, identify effective tools and procedures for

combating crime, and develop early warning and crisis management mechanisms.

The EC has made implementing the Action Plan a priority and included on the Council of Minister’s agenda for this term the establishment of a European computer crime observatory dedicated to gathering and processing information on “crimes deploying new technologies.”\(^{31}\) The planned observatory would be established within Europol, the European Police Office, along with an EU-wide research and monitoring center to provide “a strategic approach by pinpointing and applying joint standards as a basis for research into new products.”\(^{32}\) The center will be responsible for coordination between Member States, industry, and universities and will be required to promote effective investigation and prosecution methods, disseminate good practices, and provide incentives for training.

2. **Group of Eight (G-8)**

The High Tech Subgroup of the G-8 is part of the Senior Experts Group on Transnational Organized Crime established in 1995. This group is known as the “Lyon Group” since its first report was delivered at the Lyon Summit in 1996. While concerned primarily with law enforcement and developed primarily with government representatives, nearly 30 industry representatives from several countries participated in discussions held in 2000 in Paris and in 2001 in Berlin and Tokyo. Cooperation between the private and public sectors contributed to better understanding of the issues.

3. **Council of Europe (CoE)**

The Council of Europe, as well as invited “partner countries,” completed drafting a major Convention on Cybercrime in November 2001, which presently has been signed by 33 nations. While government representatives worked primarily on the text of the Convention and the accompanying Explanatory Memorandum,\(^{33}\) there was fairly extensive interaction between the public and private sectors in the U.S. during the 18 months preceding its conclusion, which produced a


\(^{33}\) The text of both the CoE Convention and the Explanatory Memorandum and other useful information on cybercrime, including links to the websites of other multilateral organizations, can be found at http://Conventions.coe.int/Treaty/EN/CadreListeTraites.htm.
document that at numerous points took practical business concerns into consideration. However, such interaction and cooperation did not change the fact that this was a negotiation among sovereigns.

4. Organization for Economic Cooperation and Development (OECD)

The OECD Working Party on Information Security and Privacy (WPISP) brings together representatives from the thirty OECD Member country governments, the private sector, and civil society to foster the emergence of solutions to build trust online. WPISP uses as a framework for building international cooperation on security the 2002 OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security.34

5. Asia Pacific Economic Cooperation (APEC)

The APEC Telecommunications and Information Working Group (APEC-TEL) brings together the government, business, and private sectors of the 21 APEC member Economies. At the 5th meeting of Ministers for the Telecommunications and Information Industries (TELMIN 5) in Shanghai, China, on May 29–30, 2002, the Ministers adopted a Statement of the Security of Information and Communications Infrastructures that, among other initiatives, called for domestic implementation of the ten measures included in the United Nations General Assembly Resolution 55/63, Combating the Criminal Misuse of Information Technologies.35 TELMIN 5 also called on APEC-TEL to give special priority to, and facilitate within, work on the protection of information and communication infrastructures. APEC-TEL has ongoing projects related to raising awareness and participated in a United States-sponsored international workshop on “Legal Frameworks for Combating Cybercrime” at TEL 26 in Moscow, Russia, in August 2002.36

6. International Telecommunications Union (ITU)

World e-Trust is a multilateral program developed by ITU37 and aimed at building secure infrastructures in developing countries to create

---

35See Shanghai Declaration at http://www.apectelmin5.org/.
digital opportunities for development. The program is a public/private cooperative effort with participation from ITU Member States, intergovernmental organizations, technology and service providers, and industry partners. ITU also organized a special workshop on Creating Trust in Critical Network Infrastructures on May 20–22, 2002, in Seoul, South Korea. The topics addressed included the need for a global approach to the dissemination of information regarding the security of critical network infrastructures, whether public or privately owned, and ways to stimulate international and regional cooperation with respect to critical network infrastructure.

B. ACTIVITIES OF NONGOVERNMENTAL ORGANIZATIONS

1. International Chamber of Commerce (ICC)

The International Chamber of Commerce (ICC) is a nonprofit organization, founded in 1919, which represents the interests of international businesses and associations. The ICC promotes an open international trade and investment system and the market economy in multiple fora. It meets regularly with ambassadors to the World Trade Organization, enjoys consultative status at the United Nations, and provides recommendations to the Group of Eight industrial countries.

In 1999, the ICC established a Cybercrime Unit in response to membership concern about the exponential growth in cybercrime. The Cybercrime Unit is responsible for keeping track of criminal methods and briefing its membership, providing expert advice on the security of information systems, identifying criminal interference in corporate computer networks, providing information, research and intelligence, and consulting with national and international law enforcement agencies.

The ICC also addresses cyber security issues in its Commission on Telecommunications and Information Technologies and its Working Group on Information Security.

---

2. Global Business Dialogue on Electronic Commerce (GBDe)

GBDe\textsuperscript{42} is an international industry-driven private sector initiative founded in 1999 to develop policies promoting global e-commerce. Its Cyber Security Working Group has focused initially on two main issues: public/private cooperation and information sharing and the promotion of mutual recognition agreements.\textsuperscript{43} In its 2000 Miami Recommendations, the GBDe noted that the process of information sharing must be consistent with national laws, recognizing that in most cases current national laws do not address the potential liability concerns of industry resulting from information received from or provided to the government.\textsuperscript{44} In the 2001 Tokyo Recommendations, the focus was further extended to the establishment of legal frameworks for the mutual recognition of certification service providers to ease the development and interoperability of digital signature and Public Key Infrastructure (PKI) programs.\textsuperscript{45}

3. Information Technology Association of America (ITAA) and World Information Technology and Services Alliance (WITSA)

WITSA\textsuperscript{46} is a consortium of 46 ICT industry associations from economies around the world; the Information Technology Association of America (ITAA) is the U.S. member of WITSA.\textsuperscript{47} WITSA is committed to encouraging public/private cooperation to enhance information security, and ITAA currently holds the chair of the WITSA Task Force on Critical Information Infrastructure. ITAA has advised the U.S. Government on information security and worked in partnership with the Government on a program to educate personal computer users on the need for cyber security.

4. Global Internet Project (GIP)

The GIP is an international group of industry executives committed to promoting industry actions that will minimize the need for government regulation in Internet-related industries.\textsuperscript{48} GIP promotes industry

\textsuperscript{47}See Information Technology Association of America, http://www.itaa.org/.
international standards for encryption and nondiscriminatory government policies on information security and encryption that allow free trade of products in this field.

5. Global Information Infrastructure Commission (GIIC)

GIIC\textsuperscript{49} is an industry organization representing both developed and developing countries and supports public/private cooperation in building the global information economy and bridging the “Digital Divide.” GIIC sponsored a survey of top global business leaders revealing that there are clear differences in interpreting the Digital Divide according to the geographic location of the business leaders. South American business leaders argue basic education reforms and privatization are needed to overcome the divide, while Asian business leaders believe culture and language are the primary cause of the divide. African business leaders understandably see poverty and the inability to gain the investment for telecommunications infrastructure as the problem, and both American and European business leaders cite information security as the major impediment for continuing development of the information economy. The GIIC attempts to address these diverging concerns in a way that unifies priorities and brings industry leaders in direct cooperation with intergovernmental organizations such as the UN and the World Bank.

C. SELECTED ACTIVITIES WITHIN SPECIFIC COUNTRIES

1. United Kingdom

The U.K. has established the National Infrastructure Security Coordination Center (NISCC) to defend critical national infrastructure from electronic attack. The NISCC includes government agencies, organizations, and private sector companies.\textsuperscript{50}

2. Canada

Canada’s Office of Critical Infrastructure Protection and Emergency Preparedness (OCIEPEP) established two partnership development divisions—Domestic Partnerships and International Partnerships.\textsuperscript{51}

\textsuperscript{49}More information, including a report on the April 2002 meeting in Beijing, is available at http://www.giic.org.

\textsuperscript{50}See http://www.niscc.gov.uk/aboutniscc/index.htm for more information about the U.K. National Infrastructure Security Coordination Center.

\textsuperscript{51}For more information, see http://www.epc-pcc.gc.ca/home/index_e.html.
3. Australia

In Australia, the National Office for Information Economy (NOIE) is the lead agency responsible for developing relationships between state and territory governments and industry. The NOIE oversees an awareness-raising program targeting the private sector. The program includes an annual summit (in five states) that brings key stakeholders from public and private sectors together to share information on e-security and national information infrastructure.

4. United States

The National Institute of Standards and Technology (NIST) is a government entity within the U.S. Department of Commerce that is heavily involved in standards setting. Currently, the FBI’s National Infrastructure Protection Center (NIPC), the U.S. Department of Commerce’s Critical Infrastructure Assurance Office (CIAO), the Computer Emergency Response Team (CERT) at Carnegie-Mellon University, and the Federal Computer Incident Response Center (FedCIRC) coordinate much of the available information relating to security vulnerabilities.

VI. Additional Resources

A. STANDARDS-SETTING BODIES

Below is a listing of important standards-setting bodies that have ongoing work pertaining to ICT security.

- American National Standards Institute (http://www.ansi.org): ANSI, founded in 1918, is a private, nonprofit organization that administers and coordinates the U.S. voluntary standardization and conformity assessment system.
- Institute of Electrical and Electronics Engineers (http://www.ieee.org): IEEE, a nonprofit, technical professional association of nearly 400,000 members in 150 countries, is a leading authority in technical areas ranging from computer engineering, biomedical technology, and telecommunications, to electric power, aerospace, and consumer electronics.
- International Standards Organizations (http://www.iso.org): ISO is a network of national standards institutes from 140
countries working with international organizations, governments, industry, business, and consumer representatives.

- **International Telecommunications Union** (http://www.itu.org): ITU, an organization within the UN system, helps governments and the private sector coordinate global telecom networks and services.

- **National Institute of Standards and Technology** (http://www.nist.gov): NIST, founded in 1901, is a nonregulatory federal agency within the U.S. Department of Commerce, whose mission is to develop and promote measurements, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.

- **Underwriters Laboratory** (http://www.ul.com): UL, founded in 1894, is an independent, not-for-profit product safety testing and certification organization.

### B. SECURITY-RELATED STANDARDS

Security-related standards reflect partnership within industry and between industry and government. The following partial list is included to underscore the need for and benefits of cooperation and partnering:

- Cryptographic Module Security Requirements—FIPS 140.
- Data Encryption (DES)—FIPS 46-3, ANSI.
- Digital Signature Standard and Secure Hash Standard (DSS/SHS)—FIPS 186-2, 180-1.
- Entity Authentication—FIPS 196, IETF.
- Key Management—FIPS 171, ANSI X9.17.
- Computer Data Authentication (MAC)—FIPS 113, ANSI.
- Public Key Infrastructure (PKI)—X.509.

### C. SELECTED WEBSITES

For more information relating to security standards, including standards relating to forensics useful in investigating computer crime, see the following websites.

- **Australian Computer Emergency Response Team** (http://www.auscert.org.au/render.html?it=2248): AUSCERT is a member of

---

FIRST and provides a single point of contact for the Australian Internet community to deal with computer security threats and prevention. This website provides a list of Australian and some international security standard protocols.

- **FIRST: Forum of Incident Response and Security Team** ([http://www.first.org/](http://www.first.org/)): FIRST is a coalition of computer security incident response teams from government, commercial, and academic organizations worldwide.


- **ISOC: Internet Society** ([http://www.isoc.org/standards](http://www.isoc.org/standards)): ISOC is the organizational home of the Internet Engineering Task Force, the Internet Architecture Board, the Internet Engineering Steering Group, and the Internet Research Task Force—the standards-setting and research arms of the Internet community.


- **OASIS** ([http://www.oasis-open.org](http://www.oasis-open.org)): OASIS (Organization for the Advancement of Structured Information Standards) develops open standards for web-based interactions through the XML standard. It has recently promulgated the Security Assertion Markup Language (SAML).

- **Records Management Institute** ([http://www.rmicanada.com/standards_e.html](http://www.rmicanada.com/standards_e.html)): RMI is a Canadian organization founded in 1952 for the purpose of exchanging information with the public. This site contains a list of links to Canadian and international computer security standards.

- **W3C—World Wide Web Consortium** ([http://www.w3c.org](http://www.w3c.org)): W3C is an organization that works on open protocols for continued evolution of the Internet. It has developed the Platform
for Privacy Preferences (P3P) as a protocol to be included in web browsers and servers to facilitate automated negotiation regarding privacy preferences.

VII. Conclusion

Businesses, governments, and individuals around the world increasingly experience the benefits of the Internet through e-commerce, e-government, and e-mail. However, the same cyber space that affords these positive opportunities is also vulnerable to those who use this capability for criminal purposes. The challenges presented by cyber attacks and cyber criminal activities require cooperation and coordination between the public and private sectors in order to share information, respond effectively to these risks, and mitigate their impact. Neither the government nor the private sector can address these problems standing alone. Awareness of, and experience gained from, such cooperation at all levels of government and industry, in various countries, and in multilateral forums will play an important role in expanding this cooperation and capability—a key objective of this Guide. Earlier chapters have addressed the substantive, jurisdictional, enforcement, and forensic aspects of Cybercrime. Help and assistance are available for this effort. To paraphrase John Donne, no person is an island.
I. Bibliography

A. CASES

Khan v. U.K., May 12, 2000, Reports of Judgments and Decisions, ECtHR, 2000-V.
Klass v. Germany, Sept. 6, 1978, 2 EHRR 214.
United States v. Middleton, 231 F.2d 1207 (9th Cir. 2000).
U.S. v. Bank of Nova Scotia, 691 F.2d 1384 (11th Cir. 1982), cert. denied,
United States v. Gorshkov, Case CR00-550C, Suppression Hearing
YAHOO!, Inc. v. La Ligue Contre Le Racisme Et L’antisemitisme, 169

B. ORGANIZATIONS
Australia’s Computer Emergency Response Team, http://www
Australia’s National Office for Information Economy, http://www
noie.gov.au.
Canada’s Office of Critical Infrastructure Protection and Emergency
Center for Education and Research in Information Assurance and
Customs CyberSmuggling Center’s website at, http://www.customs
.ustreas.gov/enforcem/cyber.htm.
Cybercrime information, including links to other multilateral
organizations, http://conventions.coe.int/Treaty/EN/projets/
FinalCybecrime.htm.
EU actions can be found at http://cybercrime-forum.cec.eu.int/default/.
Europol links to EU Member States’ national law enforcement websites, links to European institutions and international organizations, and links to other law enforcement agencies and organizations, http://www.europol.eu.int/content.htm?links/en.htm.
Information Sharing and Analysis Center—Emergency Fire Services, http://www.usfa.fema.gov/dhtml/media/02-nipc.cfm.
Inter-American Committee on Terrorism (CICTE), http://www.oas.org/juridico/english/docu2.htm.
International Information Systems Security Certification Consortium,  
Internet Fraud Complaint Center, http://www1.ifccfbi.gov/index.asp.
Interpol, Information Technology Crime—Regional Working Parties,  
Interpol, National Central Reference Points, http://www.interpol.int/Public/contact.asp.
National Security Telecommunications Advisory Committee,  
U.K. National Infrastructure Security Coordination Center,  
U.S. Department of Justice, Criminal Division, Fraud Section public web site for Internet fraud, http://www.internetfraud.usdoj.gov.

C. REFERENCE MATERIALS


Connecticut Guidelines for Searching and Seizing Computer Systems and Electronic Evidence, State of Connecticut Division of Criminal Justice and Department of Public Safety, 1999 (available by request from Computer Crimes and Electronic Evidence Unit, 278 Colony Street, Meriden, CT 06451, USA).


Dr. Dorothy E. Denning, Georgetown University, Testimony before Special Oversight Panel on Terrorism, Committee of Armed Services, U.S. House of Representatives, May 23, 2000.


“Fighting Cybercrime—What Are the Challenges Facing Europe?,”
Meeting before the European Parliament, Sept. 19, 2000,
Euremarks.htm.

Final Report of the Second Meeting of Government Experts on Cybercrime,

Final Report of the Third Meeting of Ministers of Justice or of Ministers or
Attorneys General of the Americas, Resolution of the Assembly
General: Third Meeting of the Ministry of Justice, AG/RES 1562
english/ministry_of_justice_iii_meeting.htm.

Final Report on the Meetings of Government Experts on Cyber Crime
(Preliminary Version), Permanent Council of the Organization of
EngOAS10.pdf.

Fishman and McKenna, Wiretapping and Eavesdropping, (2d Edition
1995).

Friedrich Kubler, “How Much Freedom for Racist Speech?:
Transnational Aspects of a Conflict of Human Rights,” 27 Hofstra

G8 Communiqué, 2001 Genoa Summit, Genoa, July 22, 2001,
http://www.g8.gc.ca/genoa/july-22-01-1-e.asp.

General Guidelines for Seizing Computers and Digital Evidence, State
of Maryland, Maryland State Police, Criminal Enforcement
Command, Computer Crimes Unit, Computer Forensics
Laboratory, http://www.mdsp.org/ccu/Guidelines%20%20Seizure
%20of%20Digital%20Evidence.htm.

“German Court Ruling Threatens Internet Freedom,” The Journal for

Overview,” U.S. Department of Justice, U.S. Attorney’s Bulletin,


George Sutcliffe, E-Commerce Insurance and Risk Management (2d

Global Internet Statistics: Sources & References, Global Internet
global-reach.biz/ globstats/evol.html.


Policy Statement, International Telecommunication Union, Commission on Telecommunications and Information Technologies, June 6,


U.S. Department of State, International Judicial Assistance, Notarial Services and Authentication of Documents, http://travel.state.gov (the site also lists (a) foreign embassies and consulates in the United States; and (b) U.S. embassies abroad).


**D. STATUTES AND LEGAL DOCUMENTS**


18 U.S.C. Sections 2701–2702 (U.S. access to or disclosure of stored communications information), http://www.law.cornell.edu/uscode/18/2701.html.


A/RES/55/63, “Combating the criminal misuse of information technologies,” UN General Assembly, 81st Plenary Meeting, Dec. 4,


Electronic Communications Privacy Act, 18 U.S.C. 2701 et seq.
Germany’s Criminal Procedure Code (Strafprozeßordnung, StPO), Section 100, http://www.iuscomp.org/gla/statutes/StPO.htm (English).


II. Additional Resources

A. CYBERCRIME


**B. JURISDICTION**


C. LAW ENFORCEMENT


David Reiter, Elizabeth Blumenfeld, Mark Boulding (editors), Internet Law for the Business Lawyer, Section of Business Law, American Bar Association (Chicago).


“Europe Weighs Recording All Phone Calls, Net Traffic for 7 Years,” May 17, 2001, Politech@politechbot.com.


D. SEARCH AND SEIZURE


E. PUBLIC/PRIVATE COOPERATION


F. OTHER


Peter Wolcott and Seymour E. Goodman, Is the Elephant Learning to Dance? The Diffusion of the Internet in the Republic of India, Georgia Tech Information Security Center and the Center for International Security and Cooperation, Georgia Institute of Technology and Stanford University.


William Foster and Seymour E. Goodman, The Diffusion of the Internet in China, Center for International Security and Cooperation, Stanford University, Nov. 2000.)
ABA International Cybercrime Project, 9–10
ABA Privacy and Computer Crime Committee, xxii, 2, 10
ABA Section of Science & Technology Law, Privacy & Computer Crime Committee, 1n. 2
academia, xxi, xxii, xxx, 78–79, 120
access devices, uses of for fraud, 38
access to and disclosure of stored communications data, 29–30
Action Plan to Combat High-Tech Crime, 3, 3n. 5
Agency for Information Infrastructure Protection, (AIIP), 78
air traffic control systems, 172
airline systems, 172
alcohol, Internet sale of, 37
American Bar Association
  Global Cyberspace Jurisdiction Project, 41n. 1
  International Cybercrime Project, xxi
American Convention on Human Rights, xxvii, 135, 136n. 11
American Institute of Certified Public Accountants (AICPA), 187, 187n. 28
American National Standards Institute (ANSI), 185, 194
American Society for Industrial Security, 12n. 3
Amsterdam Treaty, 106, 106n. 50
anticompetition, 181
antitrust, xxix, 181, 182n. 18, 184
antitrust laws, information sharing and, 181–182
APEC Industrial Science and Technology Working Group (IST WG), 114, 114n. 73
APEC Telecommunications and Information Working Group (APEC-TEL), 114, 114n. 73, 190
application service providers (ASPs), 171
Argentina, 51, 70n. 68
Asia-Pacific region, xxiii
  laws on crimes against communication systems, 33–34
  laws on crimes against computer systems, 24–26
  Australia, 24–25
  Japan, 25
  Singapore, 25–26
Asia-Pacific Economic Cooperation (APEC), xxiii, 15, 100, 113–114, 190
Assurance Services Development Board of the Canadian Institute of Chartered Accounts (CICA), 187
attack tools, 86
Attorneys General and Ministers of Justice and Interior of the OAS, 70, 70n. 68
audit and assessment standards, 186, 186n. 27
Australia, 24–25, 194
laws on crimes against computer systems, 24–25
Australian Computer Emergency Response Team (AUSCERT), 195–196
authorization, 165
Bahamas, bank-secrecy laws and, 54
Bank for International Settlements (BIS), xxiii, 15
Bank of Nova Scotia case example, 54, 54n. 21
Best Evidence Rule, 103
bombs, 13
Budapest, 4n. 7, 22, 20, 32n. 41, 61, 61n. 38
Business Software Alliance (BSA), 77, 77n. 87
Canada Institute of Chartered Accountants, 187
Canada International Development Agency (CIDA), 5n. 10
Canadian Charter of Rights and Freedom, 144, 144n. 40
Canadian laws on crimes against communication systems, 30–31
Canadian laws on crimes against computer content and systems, 20–21
Carnegie-Mellon University, Computer Emergency Response Team (CERT) and, 194
Center for Education and Research in Information Assurance and Security, 12n. 3
CCIPS. See Computer Crime and Intellectual Property Section
CFAA, 17–20
chain-of-custody laws, 118
chemical, biological, and nuclear security, 172
chemical plants, 172
chief information officer, 187
chief security officer, 187
child pornography, xxv, 37, 57, 63, 63n. 43, 73
child-sex tourism, 37
China (Shanghai), 190
CHIP units. See Computer Hacking and Intellectual Property units
CIAO. See Critical Infrastructure Assurance Office
CICP. See Centre for International Crime Prevention
Code of Criminal Procedure (Germany), 33
Code Red virus, 12–13, 177
Combating the Criminal Misuse of Information Technologies, 190
comity, 45, 45n. 3, 55
Common Criteria, 186, 186n. 26
Common Criteria Recognition Arrangement, 185–186, 186n. 26
Communication on Cybercrime (European Commission), 32
communication providers, xxvii, 3, 10
communications, 172
“Communications Data,” 33
communications networks, xxix, 3, 167, 183
communications, real-time interception of, 125
Computer and Telecommunications Coordinators (CTCs), 92, 92n. 12
Computer Crime and Intellectual Property Section (CCIPS), 92–93, 92n. 13
Index

Computer Data Authentication (MAC), 195
Computer Emergency Response Team (CERT), 12n. 3, 194, 194n. 53
Computer Fraud and Abuse Act (CFAA), 16–20, 16n. 10
Computer Hacking and Intellectual property (CHIP) units, 93
Computer Misuse Act of 1990 (CMA), 21–22, 21n. 19
Computer Misuse Act of 1992 (Singapore), 25–26, 25n. 27
computer science, xxviii, 166
Computer Security Institute, 12n. 3
computer-dependent infrastructures, 167
computer users and businesses, 173
computer-related forgery, 62, 62n. 42
crimes against computer systems, laws on, 16–26
controlled substances, Internet sale of, 37
crimes facilitated by computers and Internet, 34–40
crimes against computer systems, laws on, 16–26
Council Framework Decision, xxvi
Cybercrime Convention (CoE Convention), xxiv, xxvii, xxvi, 1, 4–5, 4n. 7, 21, 22, 22n. 21, 32, 32n. 42, 43, 55, 61–67, 61n. 38, 78, 96, 111
laws on crimes against communication systems, 32
laws on crimes against computer systems, 22–23
Council of Europe’s Experts Committee on Cybercrime, CCIPS and, 93
Creating Trust in Critical Network Infrastructures, 191, 191n. 38
crimes against communications systems, laws on, 26–34
Asia-Pacific, 33–34
Europe, 31–33
North America, 28–31
crimes against computer contents and systems, laws on, 16–21
Canada, 20–21
United States, 16–20
crimes against computer systems, laws on, 16–26
Asia-Pacific, 24–26
Europe, 21–24
North America, 16-21
copyright infringement, 63, 63n. 44
child pornography, 37
child-sex tourism, 37
economic espionage, 36–37
fraud, 35–36
intellectual property theft, 37
minors, enticement to sexual activity, 37
money laundering, 36
obscenity, 37
cybercrime laws, xxii–xxiii, 11–40

crimes facilitated by computers and
Internet (continued)
online securities fraud, 38
prostitution, 37
sale of regulated items, 37
use of access devices for fraud
criminal activities, 48, 83, 84, 87,
166, 170
15, 20n. 16, 21, 21n. 17, 30–31,
30n. 37, 31n. 38, 144–147,
144n. 42, 144n. 43, 145n. 44,
145n. 45, 145n. 46, 145n. 48
Criminal Procedure Code (Italy), 33
critical infrastructure, xxix, 6, 12, 19,
39, 95, 166, 167, 168–169, 171,
173, 176
Critical Infrastructure Assurance
Office (CIAO), 98, 169,
169n. 4, 194, 194n. 53
critical infrastructure protection,
xxix, 166
Critical Infrastructure Protection
Board (CIPB), 170, 170n. 5
cross-border cybercrime cases, 49–50
juveniles and, 57
cross-border searches, 59–61
Cryptographic Module Security
Requirements, 195
cryptography policy, 109
CSI/FBI Computer Crime and
Security Survey, 12–13, 82,
178, 178n. 13
customer information, 179
cyber attacks, xxviii, 181, 187, 197
cyber security cooperation,
components of, 184–188
Cyber Security Working Group, 192,
192n. 43
Cyber Smuggling Center, 73, 73n.
75, 74
cyber stalking, 56
Cybercrime Act of 2001 (Australia),
24–25, 24n. 25
cybercrime cases, jurisdictional
issues in, 42–43

data compromised, 165
Data Encryption (DES), 195
data preservation, 4, 59, 63, 64,
64n. 49, 69, 70, 79
data privacy, 183–184
Data Protection Directive
(EU), 183
data, sabotage of, 2
data security, 180
DDOS. See distributed-denial-of-
service
DEA. See Drug Enforcement
Administration
deception, 166
DefCon, 177, 177n. 12
defend against attacks, xxix, 166
degrees of threats, 167
denial-of-service attack tool, 21
Department of Homeland Security,
98, 98n. 30, 99–100
Department of Justice (U.S.), 34, 92–96, 119, 119n. 79, 162–163, 169, 181
Department of State (U.S.), 95, 96, 161, 161n. 105
Department of the Treasury, 169
developing countries, ICTs and,
xxiii, xxviii, 5–6, 15, 24
“Digital Divide,” 5, 5n. 9, 193
Digital Signature Standard and
Secure Hash Standard
(DSS/SHS), 195
digital-signature laws, 40
digital signatures, 19, 39
digital-signature laws, 40
digital technologies, 166
digitally stored evidence,
xxvii–xxviii
methodologies for collection of,
129–132
search and seizure of, 127–135
Directive Concerning the Processing
of Personal Data and the
Protection of Privacy in the
Telecommunications Sector,
31–32, 31n. 39, 58, 101
disclosure of data, 2
distance learning, 6
distributed-denial-of-service
(DDOS) attack, 12, 165
domestic investigations, 59
domestic laws, 41, 55, 59, 62, 63,
65n. 53, 73
donor community, 5, 5n. 10
droppers, 13
Drug Enforcement Administration
(DEA), 96
“dual criminality,” xxiv, 51, 72
duplication of efforts, 174
e-commerce, xxiii, 6, 7, 8, 10, 13, 15,
16, 70, 107, 109, 113, 167, 171,
192, 197
e-commerce companies, 171
Economic Crime Survey of 2001, 82
economic espionage, 2, 36–37, 93
Economic Espionage Act of 1996
(U.S.), 36–37, 36n. 53, 54,
37n. 55
eEurope 2002, 188n. 30
eEurope Action Plan, 71, 71n. 71,
107, 107n. 53, 188, 188n. 30
electric power grids, 167
Electronic Communications
Privacy Act (ECPA), 28, 54,
54n. 22
Electronic Crime Special Agent
Program (ECSAP), 97
electronic crime units, xxvi
electronic crimes, xxiv, xxvi,
xxviii, 177
Electronic Frontier: The Challenge
of Unlawful Conduct
Involving the Use of the
Internet, 34–35, 34n. 49
Electronic Frontier Foundation,
182n. 19
electronic transactions, 16
eliminative treaties, 47
encryption, 57–58, 84
GIP standards and, 193
energy grids, 172
Entity Authentication, 195
“enumerative” treaty, 47
Eurojust, 106–107, 107n. 51
Europe, 138–141
European Anti-Fraud Office
(OLAF), 107, 107n. 52
European bank of reconstruction
and Development (EBRD),
5n. 10
European Commission, 71–72
European Convention on Human
Rights (ECHR), xxvii, 135,
136, 136n. 11, 136n. 12, 138,
138n. 21, 139
European Court of Human Rights
(ECtHR), 139–141
interception of traffic data and
126n. 4
European Institute for Computer
Antivirus research, 12n. 3
European Judicial Network (EJN), 106, 106n. 48
European laws on crimes against communication systems, 31–33
Council of Europe, 32
European Union, 31–32
Germany, 33
Italy, 33
United Kingdom, 32–33
European laws on crimes against computer systems, 21–24
Council of Europe, 22–23
other CoE states, 24
United Kingdom, 21–22
European Parliament, 71, 71n. 72, 105, 105n. 42
European Police Chiefs Operational Task Force, 106, 106n. 46
European Police Office (Europol), 105–106
European Union (EU), xxiii, xxv, xxvi, 15, 31–32, 71–72, 100, 105–107, 188–189
directive concerning the processing of personal data and the protection of privacy in the telecommunications sector, 58
EU Forum on Cybercrime, 32n. 41
laws on crimes against communication systems, 31–32
European Working Party, 76, 76n. 83
Europol, 71, 189
Europol Convention, 106, 106n. 45
Europol National units (ENUs), 106 executive agreements, 75
Executive Order 13231, 170, 170n. 6
extraditable offenses, 45, 45n. 4, 46–47, 66
extradition, xxiv, 46–47, 47n. 8
extraterritorial jurisdiction, 22, 22n. 20
FAG. See Telecommunications Installation Act
Fair Credit Reporting Act, 184, 184n. 23
FBI Academy, 95, 95n. 24
Federal Bureau of Investigation, 94–96; see also FBI
Federal Communications Commission (U.S.), 29
Federal Computer Incident Response Center (FedCIRC), 194, 194n. 53
Federal Law Enforcement Training Center (FLETC), 97–98, 98n. 29
Federal Rules of Criminal Procedure, 102
Federal Rules of Evidence, 102–103
Federal Trade Commission, 74, 184
Feira European Council, 71, 71n. 71, 188, 188n. 30
Fernmeldeanlagengesetz. See Telecommunications Installation Act
Final Report on the Meetings of Government Experts on Cyber Crime, 113, 113n. 68
Financial Action Task Force (FATF), xxiii, 14–15
financial services and banking, 172
Financial Services ISAC (FS-ISAC), 175
financial systems, xxix, 167
Finland, 74, 107
FOIA. See Freedom of Information Act
firearms, Internet sale of, 37
foreign direct investment (FDI), xxii, 2, 5–6, 7, 24, 168, 172
Foreign Intelligence Surveillance Act (FISA), 29, 123n. 1
forensic examination, of electronic evidence, 132
Forensic Science Research and Training center, 95, 95n. 24
forensics, 195, 196
Forum of Incident Response and Security Team (FIRST), 196
France, 24
fraud, 2, 7, 9, 17, 25, 30, 34, 35–36, 41, 62, 74, 83, 93, 107, 166, 172, 178
use of access devices for, 38
“free rider” issue, 177
freedom of expression, 7, 10, 53n. 18
Freedom of Information Act (FOIA), 175, 182–183
Freedom of information laws, 182–183
Freeh, Louis, 15, 15n. 9
GAO, 176, 177n. 11
G-8. See Group of Eight
gas, xxix, 167, 169
general public, xxix, 166
Germany, 24, 33
German Basic Law, right of privacy and, 136, 136n. 14,
137, 137n. 17
laws on crimes against communication systems, 33
Global Business Dialogue on Electronic Commerce (GBDe),
192, 192n. 42
global cyber security, 1, 9, 185
Global Information Infrastructure Commission (GIIC), 193,
193n. 49
Global Internet, impact of on law enforcement, 81–81
Global Internet Project (GIP),
192–193, 193n. 48
global marketplace, 166
global networks, 3
Global Programme against Corruption, 112, 112n. 65
Global Programme against Trafficking in Human Beings, 112, 112n. 65
Global Programme against Transnational Organized Crime, 112, 112n. 65
government data, 172
government information systems, 172
Gramm-Leach-Bliley Act (GLBA), 183
Group of Eight (G-8), xxi, xxv, xxvi, 5, 42–43, 67–70, 67n. 63, 100,
103–104, 189
background, 67–68
countries, 1, 1n. 1
initiatives, 3–4
Meeting of Justice and Interior Ministers, 3, 3n., 103, 103n. 37
Principles and Action Plan, 69–70,
69n. 66
subgroup on high-tech crime, 68–69, 93
summit in Halifax, Nova Scotia (1995), 68
24/7 Point-of-Contact Network, 3–4, 49, 63, 93, 100, 116
Group of Eight and Council of Europe, actions by, 2–5
Council of Europe Cybercrime Convention, 4–5
G-8 initiatives, 3–4
guidelines for computer and electronic evidence search and seizure, 132–135
Canada, 134
Council of Europe, 134–135
industry bodies, 134
United States, 132–134
Health and Human Services Department (HHS), 169, 183
Health Insurance Portability and Accountability Act (HIPAA), 183
Holocaust case example, 54, 54n. 20
Homeland Security Act (HS Act) of 2002, 98–100, 98n. 31
Homeland Security Advisory System, 98
homeland security considerations, 98–100
human rights, xxvii, 3, 7, 10, 65, 104, 112
I LOVE YOU virus, 13, 16, 52, 63, 118
ICC Commission on Telecommunications and Information Technologies, 191, 191n. 41
ICC Cybercrime Unit, 191, 191n. 40
ICC Working Group on Information Security, 191, 191n. 41
ICT, xxiii, xxv, xxix, xxx, 2, 3, 5–8, 10, 11, 15, 16, 24, 36, 40, 47, 49, 81, 83, 84, 86, 87, 96, 97, 99, 103, 104, 107, 109, 111, 112, 120, 168, 170–171, 177, 185, 186, 187, 192, 194
ICT systems, 11
developing countries and, 5–6
money laundering and, 36
identity theft, 35, 35n. 51
incidents, 167, 175, 179, 187
industry-government partnerships, 195
Information Analysis and Infrastructure Protection (IAIP), 98
information and communication technology (ICT), xxiii, 2, 81
“information is power,” 166
“information revolution,” 166
information sharing, xxv, xxix–xxx, 82, 89, 92, 98, 108, 120, 121
benefits of, 176–178
laws that impede, 181–184
potential risks of, 178–181
disclosure of proprietary or sensitive information, 178–179
disruption of business operations, 179–180
liability, 180–181
relocation of resources, 179
risks to organization’s reputation/stock price, 179
information sharing and analysis centers (ISACs), xxix–xxx, 77–78, 77n. 88, 170, 174–176
Information Society Directorate General of the European Commission, 196
Information Systems Audit Control Association (ISACA), 187, 187n. 28
information technology, 76, 77, 89, 110, 112, 166, 167, 168, 170, 171–172, 175, 186, 196
Information Technology Association of America (ITAA), 77, 192, 192n. 47
information technology industry, 171–172
Information Technology ISAC, 175, 175n. 9
InfraGard program, 95, 95n. 23, 99, 175–176, 176n. 10
infrastructure, 168
management, 173–174
infrastructure attacks, 8
infrastructure sectors, 168, 169
Institute of Electrical and Electronics Engineers (IEEE), 194
Institute of Internal Auditors, 187, 187n. 28
insurance, xxx, 168, 181, 187–188
insurance, cyber incidents and, 187–188
intellectual property, theft of, 36–37
intellectual property violations, 74
Inter-American Committee on Terrorism (CICTE), 113, 113n. 70
Inter-American Development Bank (IADB), 5n. 10
interjurisdictional networks, 72–79
internal auditor, 187
International Chamber of Commerce Cybercrime Unit, 76n. 85
International Chamber of Commerce (ICC), 76, 191, 191n. 39
International Computer Crime Conference (Oslo), 84–85
International Computer Security Association, 12n. 3
International cooperation, global cybercrime problems and, 8–9
International Covenant on Civil and Political Rights, 135, 136n. 11
International Criminal Police Organization (Interpol), 108, 108n. 56
International Cybercrime Project, 1–2, 1n. 2
scope of, 9–10
International Engineering Task Force (IETF), 185
International Guide to Combating Cybercrime, xxi, 2
International human rights protection of privacy, 135–136
International Information Systems Security Certification Consortium, 12n. 3
International Law Enforcement Cooperation Initiatives, 103–114
Asia-Pacific Economic Cooperation, 113–114
Council of Europe, 104
European Union, 105–107
Group of Eight, 103–104
Interpol, 108
Organization of American States, 113
Organization for Economic Cooperation and Development, 109–110
United Nations, 110–113
international legal assistance, 43–49
International Marketing Supervision Network (IMSN), 74, 74n. 78, 79
International Narcotics and Law Enforcement Affairs (INL), Bureau (U.S.), 96
international searches, legal concerns for, 159–163
International Standards Organization (ISO), 185, 194–195
international task forces, 74–75
International Telecommunications Union (ITU), 190–191, 190n. 37, 195
international trade, 191
Internet, xxi, xxii, xxiv, xxviii, 1, 2, 3, 5, 6, 8, 9, 12, 13, 14, 16, 26, 34–39, 42, 52, 53–54, 55, 58, 63, 70, 73, 74, 81–87, 92, 96, 107, 112, 119, 126, 129, 132, 143, 162, 166, 171, 177, 193, 196, 197
Internet backbone providers, 171
Internet fraud, 35–36
Internet Fraud Complaint Center, 35n. 50, 94, 94n. 21
Internet Protocol (IP), 81
Internet service providers (ISPs), 9, 171, 172, 188
Internet Society (ISOC), 196
Internet-related stock fraud, 38
Interpol, 75–76, 75n. 82, 76n. 83, 76n. 84, 84, 108, 108n. 56, 162
Italy, 33, 67, 103, 112
laws on crimes against communication systems, 33
ITU. See International Telecommunications Union
Japan, 4, 25, 33–34, 61, 67, 67n. 63, 104
Diet, wiretapping and, 34, 34n. 47
laws on crimes against communication systems, 33–34
laws on crimes against computer systems, 25
Japanese Law on Communication Interception During Criminal Investigations, 34, 34n. 48
joint responses, xxix, 166
judicial and statutory standards for access to stored communications and traffic data U.S. Model, 147–150
judicial and statutory standards for interception of communications and traffic data, 137–147
Canada, 144–147
Europe, 138–141
United States, 141–144
judicial and statutory standards for search and seizure of stored data, Canadian model, 150–155
jurisdiction, 41–80
conflicts of law, 49–59
cybercrime-related jurisdictional concerns, 59–79
international legal assistance, 43–49
jurisdictional issues, xxiv–xxv, 49–59
general, 41–42
in cybercrime cases, 42–43
juveniles, jurisdiction over, 57
key escrow, 40
Key Management, 195
Klass v. Germany, 140n. 24
Kopp v. Switzerland, 140n. 23
laboratories, 172
impact of cybercrime on, 84–114
practical considerations, 114–120
redefining, 82–84
lead agencies, 169
legal framework, xxi, xxv, xxvi, xxvii, 1, 6, 8, 9, 22, 40, 50, 55, 83, 91, 92, 103, 107, 115, 121, 171, 173, 192
“Legal Frameworks for Combating Cybercrime,” 190, 190n. 36
letter of exemption, 181
Letters Rogatory process, xxiv, 42, 46, 46n. 6, 47–48, 116
“list” treaty, 47
“Love Bug,” 52n. 17
Lyon Group, 68, 189
Lyon Summit, 68, 189
Maastricht Treaty, 106
“malware,” 12, 14
management oversight, ICT security and, 187
Memoranda of Understanding (MOUs), 75
Mexico–U.S.–Canada Health Care Fraud Task Force, 75
Microsoft, 77, 118
Ministers for the Telecommunications and Information Industries (TELMIN), 190
Mischief in Relation to Data
(Criminal Code of Canada), 20–21, 20n. 16
mischievous intent, 166
MLATs. See Mutual Legal Assistance Treaties
money laundering, 35–36
multilateral initiatives, 61–72
Mutual Legal Assistance Treaties (MLATs), xxiv, 42, 44–46, 44n. 2, 50, 51, 100–102

National Advocacy Center (NAC), 94
National Association of Corporate Directors (NACD), 187, 187n. 28
National Central Bureaus, 108
national constitutions, right of privacy and, 136–137, 137n. 15
National Cybercrime Training Partnership (NCTP), 93–94, 94n. 17
National Infrastructure Protection Center (NIPC), 12n. 3, 19, 19n. 14, 95, 95n. 22, 98, 169–170, 170n. 5, 194, 194n. 53
National Infrastructure Security Coordination Center (NISCC), 193, 193n. 50
National Institute of Justice (NIJ), 89
National Institute of Standards and Technology (NIST), 185, 185n. 25, 194, 194n. 53, 195
National Office for Information Economy (NOIE), 194, 194n. 52
national security, xxix, 7, 167, 176
National Strategy to Secure Cyberspace, 167, 167n. 2
National White Collar Crime Center, 94, 94n. 21
NCB. See National Central Bureaus
NCTP. See National Cybercrime Training Partnership
Netcraft Web Server Survey, 81, 81n. 1
network security, 8, 166, 187
networked world, establishment of jurisdiction in, 55–57
New York Electronic Crimes Task Force (NYECTF), 97, 97n. 27
NGOs. See nongovernmental organizations
NIJ. See National Institute of Justice
NIMDA worm, 177
NIPC. See National Infrastructure Protection Center
NIST’s Computer Security Resource Center, 12n. 3, 196
NIST’s Information Technology Laboratory, 196
nongovernmental organizations (NGOs), xxi, xxvii, xxx, 2, 120, 171
North American laws on crimes against communications systems, 28–31
Canada, 30–31
United States, 28–30
North American laws on crimes against computer content and systems, 16–21
Norway, 56, 74, 84
nuclear facilities, 172
OAS. See Organization of American States
OASIS. See Organization for the Advancement of Structured Information Standards
OECD. See Organization for Economic Cooperation and Development
Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP), 193, 193n. 51
Office of International Affairs (OIA), 45–46
oil, xxix, 167, 169
Okinawa Charter on Global Information Society, 4, 4n. 6
Okinawa Summit, 4
OLAF. See European Anti-Fraud Office
Omnibus Crime Control and Safe Streets Act, 102
online securities fraud, 38
open-access global marketplace, 166
“Operation Buccaneer,” 74
“Operation Kinderschutz,” 73
Organization for Economic Cooperation and Development (OECD), xxiii, 14, 15, 100, 109–110, 190
Committee for Information, Computer and Communications Policy (ICCP), 109
Cryptography Policy Guidelines and the report on Background and Issues of Cryptography Policy, 109, 109n. 57
Guidelines for the Security of Information Systems, 110, 110n. 58
Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, 190, 190n. 34
Working Party on Information Security and Privacy (WPISP), 110, 190
Organization for the Advancement of Structured Information Standards (OASIS), 196
Organization of American States (OAS), 70–71, 70n. 68, 100, 113
cybercrime project, CCIPs and, 93
Overseas Prosecutorial Development Assistance and Training (OPDAT) unit, 95
P3P. See Platform for Privacy Preferences
packet switching, 9
pen registers, xxii, 14, 27, 27n. 28, 28n. 31, 30, 48, 143
penetration testing, 186
performance-based operating guidelines, 185
personal computer, 167, 192
pharmaceuticals, 73
Philippines, I LOVE YOU virus and, 15, 52, 52n. 17, 118
physical security, 187
Platform for Privacy Preferences (P3P), 196–197
Ponzi schemes, 38
Presidential Decision Directive 63 (PDD-63), 169, 169n. 3
prescription drugs, Internet sale of, 37
Principles to Combat High-Tech Crime, 3, 3n. 5, 104, 104n. 39
Privacy Act, 184, 184n. 22
“private communications,” 144, 144n. 42
private organizations, xxix, 166, 167, 173, 178
private sector, xxi, xxii, xxv, xxvii, xxviii, xxix, xxx, 1, 2, 10, 43, 76, 78, 89, 90, 92, 96, 97, 99, 118, 120, 121, 166, 168, 170, 171, 173, 174, 175, 176, 179, 181, 182, 183, 184, 185, 189, 190, 192, 194, 197
professional criminal, 167
Proposal for a Council Framework Decision on attacks against information systems, 72, 72n. 74
proprietary data, xxix, 166
prostitution, 37
“protected computers,” xxii
public key infrastructure (PKI), 40, 192, 195
public/private cooperation, xxviii–xxx, 165–197
analysis, 173–184
components of cyber security cooperation, 184–188
international efforts, 188–194
preliminary issues, 168–173
real-time interceptions, xxvii
of communications, 125
of traffic data, 125–126, 125n. 3, 143–144
Records Management Institute, 196
regulated items, sale of, 37
regulatory mindset, 173
Regulation of Investigatory Powers Act (RIPA), 32–33, 32n. 43
Reno, Janet, G-8 counterparts and, 69
risk management, 184–188
Russia, 60, 155
sabotage of data, 2
sale of regulated items, 37
San Diego Supercomputer Center (SDSC), 51
“script kiddies,” xxviii, 165, 165n. 1, 177
search and seizure, xxvii–xxviii, 123–163
of digitally stored evidence, 127–135
jurisdictional issues, 155–159
legal considerations, 135–163
types of, 124–127
Secret Service. See U.S. Secret Service
secure operating environment, 171
Security Assertion Markup Language (SAML), 196
security audits, 186–187
security breaches, xxix, 166, 180, 182, 188
security personnel, 181
security practices, 168, 175
security-related standards, 195
security researchers, xxix, 166
security standards, 168, 185, 195, 196
Senior Experts Group on Transnational Organized Crime, 189
September 11, 2001, 14, 16–17; see also Terrorism
sexual activity, enticing minors to engage in, 37
Shanghai Declaration, 190n. 35
share resources, xxii, xxix, 166
shareholder values, 187
Singapore laws on crimes against computer systems, 25–26
small and medium sized enterprises (SMRs), 6
smart cards, 186
South Africa, 4, 61
standards-setting bodies, 194–195
Stanford Draft International Convention to Enhance Protection from Cyber Crime and Terrorism, 78–79, 78n. 89
State Department. See Department of State
Statement of the Security of Information and Communications Infrastructures, 190
steganography, 13, 84, 84n. 7
stored data, access to by search and seizure, 126
stored digital evidence, xxvii–xxviii
Strategic Information and Operations Center (SIOC), 95
subpoena, xxviii, 29, 44, 45, 48, 91, 115, 124, 149, 160
compelled disclosure of stored data by, 127
Switzerland, 51
Tampere European Council, 71, 71n. 70, 107
technical expertise, law enforcement and, 48–49
technology neutrality, 40
teenage hacker, 167
Telecommunications Act (Germany), 33, 33n. 44
Telecommunications Business Law (Japan), 33–34, 33n. 45
Telecommunications Installation Act (Germany), 33, 33n. 44
Telecommunications ISAC (Telecom-ISAC), 175
Telekommunikationsgesetz. See Telecommunications Act
terrorism, 14, 16–17, 98, 99, 105, 113
Department of Homeland security and, 98
The Europol Computer System (TECS), 106
theft, 50, 166, 178
theft of intellectual property, 36–37
think tanks, 78–79
TKG. See Telecommunications Act
Tokyo Recommendations, 192
traffic data, real-time interception of, 125–126, 125n. 3, 143–144
traffic management systems, 172
transborder searches, 155–158
trap-and-trace, xxii, 14, 27, 27n. 28, 28, 28n. 31, 30, 48, 143
Trojan horse programs, 13
Trust, xxix
unauthorized access, 2, 14
Unauthorized Computer Access Law of 1999 (Japan), 25, 25n. 26
Unauthorized Use of Computer (Criminal Code of Canada), 20, 20n. 15
Underwriters Laboratory (UL), 195
UNICRI. See United Nations Interregional Criminal Justice and Research Institute
United Kingdom, 21–22, 32–33
Computer Misuse Act, 21, 21n. 19
encryption laws and, 57–58
laws on crimes against communication systems, 32–33
laws on crimes against computer systems, 21–22
National Infrastructure Security Coordination Center (NISCC), 193, 193n. 50
United Nations, xxiii, xxvi, 5, 5n. 10, 15, 100, 110–113
Centre for International Crime Prevention (CICP), 111, 112n. 62
Congress on the Prevention of Crime and the Treatment of Offenders, 113, 113n. 67
Convention Against Transnational Organized Crime, 112, 112n. 66
Crime and Justice Information Network (UNCJIN), 112, 112n. 64
General Assembly Resolution 55/63, 190
International Narcotics Control Board (INCB), 96, 96n. 25
Interregional Criminal Justice and Research Institute (UNICRI), 112, 112n. 63
Office for Drug Control and Crime Prevention, 111–112
United States, 28–30, 194
U.S. Agency for International Development (USAID), 5, 5n. 10
U.S.–Canada Telemarketing Fraud Task Force, 75
U.S. Computer Fraud and Abuse Act, 24
U.S. Constitution, Fourth Amendment to, 136, 136n. 13, 137, 137n. 16, 141
<table>
<thead>
<tr>
<th>Entry</th>
<th>Page Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S. Customs Service Cyber-Smuggling Center</td>
<td>73, 73n. 75, 97, 97n. 28</td>
</tr>
<tr>
<td>U.S. Department of Commerce</td>
<td>194, 195</td>
</tr>
<tr>
<td>U.S. Department of Justice</td>
<td>45</td>
</tr>
<tr>
<td>U.S. Electronic Communications Privacy Act</td>
<td>58</td>
</tr>
<tr>
<td>U.S. Federal Trade Commission</td>
<td>74</td>
</tr>
<tr>
<td>U.S. Food and Drug Administration</td>
<td>73</td>
</tr>
<tr>
<td>U.S. Food, Drug, and Cosmetic Act (FDCA)</td>
<td>73</td>
</tr>
<tr>
<td>U.S. laws on crimes against communication systems</td>
<td>28–30</td>
</tr>
<tr>
<td>U.S. laws on crimes against computer content and systems</td>
<td>16–20</td>
</tr>
<tr>
<td>U.S. National Institute of Justice (NIJ)</td>
<td>89</td>
</tr>
<tr>
<td>U.S. President’s Working Group on Unlawful Conduct on the Internet</td>
<td>8, 84n. 6</td>
</tr>
<tr>
<td>U.S. Secret Service</td>
<td>96–98, 99, 133</td>
</tr>
<tr>
<td>U.S. Securities and Exchange Commission (SEC)</td>
<td>75</td>
</tr>
<tr>
<td>U.S. wiretap law</td>
<td>28–29, 28n. 33</td>
</tr>
<tr>
<td>United States v. Middleton</td>
<td>18n. 12</td>
</tr>
<tr>
<td>Universal Covenant on Civil and Political Rights</td>
<td>xxvii</td>
</tr>
<tr>
<td>Universal Declaration of Human Rights</td>
<td>xxvii, 135, 136n. 10</td>
</tr>
<tr>
<td>USA PATRIOT Act</td>
<td>17, 17n. 11, 22, 29n. 35, 36, 48, 183–184</td>
</tr>
<tr>
<td>virtual nature of cybercrime</td>
<td>86–87</td>
</tr>
<tr>
<td>viruses</td>
<td>xxvii, 2, 4, 12–13, 14, 16, 21, 50, 52, 81, 83, 165, 171, 173, 189, 180</td>
</tr>
<tr>
<td>Virus Exchanges</td>
<td>177</td>
</tr>
<tr>
<td>vulnerabilities</td>
<td>xxix, 7, 19, 77, 81, 85, 86, 89, 93, 98, 99, 166, 167, 168, 169, 172, 173, 174, 175, 176, 177, 181, 182, 184, 185, 194</td>
</tr>
<tr>
<td>W3C. See World Wide Web Consortium</td>
<td></td>
</tr>
<tr>
<td>warrant</td>
<td>29, 31, 34, 48, 56</td>
</tr>
<tr>
<td>weakest link</td>
<td>1, 8</td>
</tr>
<tr>
<td>web defacement</td>
<td>2</td>
</tr>
<tr>
<td>web-jacking</td>
<td>13</td>
</tr>
<tr>
<td>Wire Telecommunications Law (Japan)</td>
<td>33–34, 34n. 46</td>
</tr>
<tr>
<td>wiretaps</td>
<td>xxii, 27, 28–29, 28n. 30</td>
</tr>
<tr>
<td>laws against</td>
<td>14</td>
</tr>
<tr>
<td>WITSA Task Force on Critical Information Infrastructure</td>
<td>192</td>
</tr>
<tr>
<td>Working Party on Information Security and Privacy (WPISP)</td>
<td>190</td>
</tr>
<tr>
<td>World Bank Group</td>
<td>5, 5n. 10</td>
</tr>
<tr>
<td>World e-Trust</td>
<td>190–191</td>
</tr>
<tr>
<td>World Information Technology and Services Alliance (WITSA)</td>
<td>76–77, 76n. 86, 192, 192n. 46</td>
</tr>
<tr>
<td>World Trade Organization (WTO)</td>
<td>xxiii, 15</td>
</tr>
<tr>
<td>International Chamber of Commerce and</td>
<td>191</td>
</tr>
<tr>
<td>World Wide Web Consortium</td>
<td>196–197</td>
</tr>
<tr>
<td>worms</td>
<td>13</td>
</tr>
<tr>
<td>Yahoo! case example</td>
<td>53, 53n. 19, 55, 55n. 24</td>
</tr>
</tbody>
</table>