Draft International Convention To Enhance Protection from Cyber Crime and Terrorism

Preamble

The States Parties to this Convention,

Acknowledging that developments in science and technology have enabled unprecedented transnational communications through information infrastructures;

Affirming the worldwide benefits enabled by those infrastructures;

Understanding the growing reliance and dependence of persons and governments upon proper operation of information infrastructures and their growing interdependence;

Recognizing the vulnerability of information infrastructures to attacks and improper utilization;

Considering the potentially grave consequences of attacks and improper utilization to persons and governments worldwide, including failures of systems and damage to critical infrastructure, economic losses, and interruption of communications;

Resolving that there is a need to protect transnational information infrastructures from attacks and improper utilization and to deter such conduct by means of appropriate penalties and technology;

Mindful of the limitations of unilateral approaches;

This Draft Convention was prepared by Abraham D. Sofaer, Gregory D. Grove, and George D. Wilson.

Mindful also of the need to ensure appropriate protection of privacy, freedom of communication, and other human rights;

Desiring active international cooperation through voluntary and mandatory measures effectively to investigate and prosecute cyber criminals and terrorists and to develop technological standards and practices to enhance cyber security;

Desiring also the establishment of a specialized agency designed to marshal the expertise to achieve the voluntary and mandatory objectives of this Convention, through a structure based on voluntary, private-sector activities, expertise, and involvement;

Convinced that there is an emerging consensus regarding certain conduct that should be prosecuted as criminal, as well as regarding the need for agreed standards and practices to enhance security; and

Recognizing the need to ensure that all cooperating states should have the technological capacities required for participating in and benefiting from advances in communication, and that all feasible assistance should be provided by technologically advanced states;

Have agreed as follows:

Article 1
Definitions and Use of Terms

For the purposes of this Convention:

1. "cyber crime" means conduct, with respect to cyber systems, that is classified as an offense punishable by this Convention;

2. [Not used]

3. "information infrastructure" and "cyber system" mean any computer or network of computers used to relay, transmit, coordinate, or control communications of data or programs;

4. "data" is information or communications content, including speech, text, photographs, sound, video, control signals, and other formats for information or communications;

5. a "program" is an instruction or set of instructions intended or designed to cause a computer or network of computers to manipulate data, display

data, use data, perform a task, perform a function, or any combination of these;

6. "transnational information infrastructures" means information infrastructures with component parts physically present in the territory of two or more States Parties;

7. "critical infrastructures" are the interconnected networks of physical devices, pathways, people, and computers that provide for timely delivery of government services; medical care; protection of the general population by law enforcement; firefighting; food; water; transportation services, including travel of persons and transport of goods by air, water, rail, or road; supply of energy, including electricity, petroleum, oil and gas products; financial and banking services and transactions; and information and communications services;

8. a "person" may be any of the following: (a) a human being or (b) a corporation or business organization recognized as a legally separate entity under the governing domestic law of a State Party or (c) any other legally recognized entity capable of performing or contributing to the conduct prohibited by this Convention;

9. "legally recognized authority" is authority under a governing State Party's domestic law for persons to enter into private places, to examine private papers, to observe private communications, or to engage in other legally authorized investigative activities;

10. "legally recognized permission" or "legally recognized consent" is permission recognized under a governing State Party's domestic law (when given by a person with a legally recognized interest in a place, tangible property, or intangible property) to enter into private places, to examine private papers, to intercept private communications, or to engage in other legally authorized investigative activities;

11. "misrouting" of communications content or data means intentionally changing or manipulating the ordinary operation of an information infrastructure with the purpose of delaying or diverting the delivery of a protected packet en route to its intended destination, or with knowledge that such delay or diversion will result;

12. a "protected packet" is an assembly of data used to convey communications content through a transnational information infrastructure, conform-

ing to an international standard for transmission of data established by the Internet Engineering Task Force (IETF) or other widely accepted process;

13. a "treaty offense" is conduct prohibited by multilateral treaty, convention, or agreement (other than this Convention) for which an individual may be punished under the governing domestic law implementing the terms of that treaty, convention, or agreement.

Article 2
Enactment of Domestic Laws

Each State Party shall adopt such measures as may be necessary:

1. to establish as criminal offenses under its domestic law the conduct set forth in Articles 3 and 4;

2. to make such conduct punishable by appropriate penalties that take into account its potentially grave consequences, including possible imprisonment for one year or more; and,

3. to consider for prompt implementation through domestic laws all standards and recommended practices proposed by the Agency for Information Infrastructure Protection (AIIP) pursuant to Article 12.

Article 3
Offenses

1. Offenses under this Convention are committed if any person unlawfully and intentionally engages in any of the following conduct without legally recognized authority, permission, or consent:

(a) creates, stores, alters, deletes, transmits, diverts, misroutes, manipulates, or interferes with data or programs in a cyber system with the purpose of causing, or knowing that such activities would cause, said cyber system or another cyber system to cease functioning as intended, or to perform functions or activities not intended by its owner and considered illegal under this Convention;

(b) creates, stores, alters, deletes, transmits, diverts, misroutes, manipulates, or interferes with data in a cyber system for the purpose and with the effect of providing false information in order to cause substantial damage to persons or property;

(c) enters into a cyber system for which access is restricted in a conspicuous and unambiguous manner;

(d) interferes with tamper-detection or authentication mechanisms;

(e) manufactures, sells, uses, posts, or otherwise distributes any device or program intended for the purpose of committing any conduct prohibited by Articles 3 and 4 of this Convention;

(f) uses a cyber system as a material factor in committing an act made unlawful or prohibited by any of the following treaties: (i) Convention on Offenses and Certain Other Acts Committed on Board Aircraft, September 14, 1963, 20 U.S.T. 2941 [Tokyo Convention]; (ii) Convention for the Suppression of Unlawful Seizure of Aircraft (Hijacking), December 16, 1970, 22 U.S.T. 1641 [Hague Convention]; (iii) Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation (Sabotage), September 23, 1971, 24 U.S.T. 564 [Montreal Convention]; (iv) International Convention Against the Taking of Hostages, December 17, 1979, T.I.A.S. 11081 [Hostages Convention]; (v) International Convention for the Suppression of Terrorist Bombings, December 15, 1997, 37 I.L.M. 249 [Terrorist Bombings Convention]; (vi) United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, December 20, 1988, T.IA.S., 20 I.L.M. 493 [Vienna Convention on Narcotics]; (vii) International Maritime Organization Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation [Maritime Terrorism Convention], March 10, 1988, IMO Doc. SUA/CON/15/Rev.1, 1993 Can. T.S. No. 10.

(g) engages in any conduct prohibited under Articles 3 and 4 of this Convention with a purpose of targeting the critical infrastructure of any State Party.

2. Purpose, intent, or knowledge with respect to the crimes set forth in paragraph 1 of this section may be inferred from objective factual circumstances.

Article 4
Attempts, Aiding and Abetting, Conspiracy

An offense under this Convention is committed if any person unlawfully and intentionally:

1. attempts to engage in any conduct prohibited in Article 3;

2. aids or abets others in engaging or attempting to engage in any conduct prohibited in Article 3; or

3. conspires with others to engage in any conduct prohibited in Article 3.

Article 5
Jurisdiction

1. Each State Party to this Convention shall take such measures as may be necessary to establish its jurisdiction over the offenses set forth in Articles 3 and 4 in the following cases:

(a) when the offense is committed in the territory of that State or on board a ship, aircraft, or satellite registered in that State or in any other place under its jurisdiction as recognized by international law;

(b) when the alleged offender is a national of that State;

(c) when the alleged offender is a stateless person whose primary residence is in its territory;

(d) when the alleged offender is present in its territory and it does not extradite such person pursuant to this Convention.

2. Each State Party to this Convention may take such measures as may be necessary to establish its jurisdiction over the offenses set forth in Articles 3 and 4 in the following cases:

(a) when the offense is committed with intent or purpose to harm that State or its nationals or to compel that State to do or abstain from doing any act; or

(b) when the offense has substantial effects in that State.

3. This Convention does not exclude any criminal jurisdiction exercised in accordance with domestic law, including any domestic law giving effect to Articles 3 and 4, or any criminal jurisdiction established pursuant to any other bilateral or multilateral treaty.

4. Each State Party will exercise its rights and fulfill its obligations under this Convention to the extent practicable in accordance with the following priority of jurisdiction: first, the State Party in which the alleged offender was physically present when the alleged offense was committed; second, the State Party in which substantial harm was suffered as a result of the alleged offense; third, the State Party of the alleged offender's dominant nationality; fourth, any

State Party where the alleged offender may be found; and fifth, any other State Party with a reasonable basis for jurisdiction.

Article 6
Mutual Legal Assistance

1. States Parties shall adopt such measures as are necessary to enable themselves to afford one another the widest measure of mutual legal assistance on an expedited and continuous basis (within conditions prescribed by treaties, domestic laws, or regulations concerning such assistance) in investigations, extraditions, prosecutions, and judicial proceedings brought in respect of the offenses set forth in Articles 3 and 4, including assistance for the following purposes:

(a) identifying and tracing attacks upon cyber systems by electronic and other means;

(b) locating or identifying persons;

(c) taking statements from persons;

(d) executing searches and seizures by electronic and other means;

(e) examining objects and sites;

(f) securing and exchanging information and evidentiary items, including documents and records; and,

(g) transferring persons in custody.

2. Requests for assistance will be made in accordance with arrangements under existing agreements between or among the States Parties involved, or through Central Authorities designated by States Parties in ratifying this Convention. Requests made for emergency assistance will be dealt with by response teams that function as necessary on a continuous basis.

3. States Parties shall promote appropriate methods of obtaining information and testimony from persons who are willing to cooperate in the investigation and prosecution of offenses established in Articles 3 and 4 and shall, as appropriate, assist each other in promoting such cooperation. Such methods of cooperation may include, among other things: granting immunity from prosecution to a person who cooperates substantially with law enforcement authorities in investigations, extraditions, prosecutions, and judicial proceedings; considering the provision by an accused person of substantial coopera-

tion as a mitigating factor in determining the person's punishment; and entering into arrangements concerning immunities or nonprosecution or reduced penalties.

4. Any physical property of substantial intrinsic value seized by a State Party that is later delivered pursuant to the request of a prosecuting State Party to facilitate the prosecution of a suspected offense shall, upon request within a reasonable time after final resolution of all proceedings of prosecution and appeal in the courts of the prosecuting State Party, be returned to the State Party that seized the property for disposition according to the domestic laws of that State Party.

5. States Parties shall be free to engage in reasonable, electronic methods of investigation of conduct covered by Articles 3 and 4 of this Convention, over which they have jurisdiction to prosecute under Article 5, even if such conduct results in the transfer of electronic signals into the territory of other States Parties. A State Party aware that its investigative efforts will likely result in such transfers of electronic signals shall as soon as practicable inform all affected States Parties of such efforts.

6. States Parties shall consider for prompt implementation through law all standards and recommended practices adopted and proposed by the AIIP pursuant to Article 12 as methods for enhancing mutual legal assistance provided under this Article 6.

7. States Parties agree to extend on a voluntary basis cooperation in all possible areas of activity bearing upon mutual legal assistance, both individually and through efforts under the auspices of the AIIP or other governmental and nongovernmental entities.

Article 7
Extradition

1. Offenses under the domestic laws of each State Party concerning any conduct set forth in Articles 3 and 4 shall be deemed to be included as extraditable offenses in any extradition treaty existing between or among States Parties. States Parties undertake to include such offenses as extraditable offenses in every extradition treaty subsequently concluded between them; however, failure to include these offenses in such treaties shall not affect the obligations undertaken herein.

2. If a State Party that makes extradition conditional on the existence of a

treaty receives a request for extradition from another State Party with which it has no extradition treaty, it may consider this Convention as the legal basis for extradition in respect of the offenses covering conduct set forth in Articles 3 and 4. Extradition shall remain subject to any other requirement of the law of the requested State.

3. States Parties that do not make extradition conditional on the existence of a treaty shall recognize offenses covering the conduct set forth in Articles 3 and 4 as extraditable offenses as between themselves, subject to any other requirement of the law of the requested State.

4. Offenses covering the conduct set forth under Articles 3 and 4 shall to that extent be treated, for the purpose of extradition between States Parties, as if they had been committed in the place in which they occurred, and also in the territories of the State or States required or authorized to establish their jurisdiction under Article 5.

5. When extradition is requested by more than one requesting State Party, the requested State Party shall respond to such requests in accordance with the priorities for jurisdiction set out in Article 5, paragraph 4.

Article 8
Prosecution

1. The State Party in the territory of which an alleged offender is found shall, if it does not extradite such person, be obliged, without exception and whether or not the offense was committed in its territory, to submit the case without delay to competent authorities for the purpose of prosecution, through proceedings in accordance with the laws of that State. Those authorities shall pursue such prosecutions in the same manner as other serious offenses under the laws of that State. If a State Party is unable or unwilling to prosecute such cases, it must promptly inform the original requesting State Party or States Parties.

2. A requesting State Party may prosecute an alleged offender over whom it secures jurisdiction through extradition only for crimes specified in its extradition request and found legally sufficient by the requested State Party, unless the requested State Party agrees to permit prosecution for additional offenses.

Article 9
Provisional Remedies

1. Upon the request of a State Party based upon its reasonable belief that a named suspected offender engaged in conduct covered by this Convention may be found in the territory of a requested State Party, the requested State Party undertakes to apprehend the named suspected offender if found in its territory and hold the suspected offender for up to a maximum of ten (10) days, during which period the requesting State Party will supply information sufficient to show cause for continued detention pending the resolution of its request for extradition.

2. Upon the request of a State Party based upon its reasonable belief that conduct covered by Articles 3 and 4 of this Convention has occurred, and that evidence of such conduct is present in the stored data contained in cyber systems located within the territory of a requested State Party, the requested State Party will attempt to preserve or to require preservation of the stored data in such cyber systems for a reasonable period to permit the requesting State Party to supply information sufficient to show adequate cause for release of all or part of the preserved stored data to the requesting State Party.

3. States Parties shall consider for prompt implementation through national law all standards and recommended practices adopted and proposed by the AIIP pursuant to Article 12 as methods for enhancing the capacity of States Parties to advance this Convention's purposes through provisional remedies.

Article 10
Entitlements of an Accused Person

1. Any person detained by a State Party pursuant to one or more of Articles 3, 4, 5, 6, 7, 8, or 9 shall be entitled, in addition to rights extended under the national law of such State Party, to:

(a) communicate without unnecessary delay with the nearest appropriate representative of the State of which that person is a national or which is otherwise entitled to protect that person's rights or, if that person is stateless, the State of that person's primary residence;

(b) be visited by a representative of that State;

(c) have a representative of that State physically present to observe any legal proceedings that may result in punishment; and,

(d) be informed promptly after detention of that person's entitlements under subparagraphs (a), (b), and (c) of this Article 10.

2. States Parties shall not deny any person, or impair in any way, the entitlements described in paragraph 1.

Article 11
Cooperation in Law Enforcement

States Parties shall cooperate closely with one another through their law enforcement agencies in preventing any conduct set forth in Articles 3 and 4, by among other things:

1. taking all practicable measures to prevent preparations in their respective territories for the commission of such conduct within or outside their territories;

2. exchanging information and coordinating the taking of administrative and other measures as appropriate to prevent commission of such conduct; and,

3. considering for prompt implementation all standards and recommended practices adopted and proposed by the AIIP pursuant to Article 12 as methods for deterring and preventing the crimes covered by this Convention.

Article 12
Agency for Information Infrastructure Protection (AIIP)

The States Parties hereby establish, and agree to make operational as soon as practicable after the effective date of this Convention, the Agency for Information Infrastructure Protection (AIIP), an international agency composed of all States Parties as Members, and consisting of an Assembly, a Council, a Secretariat managed by a Secretary General, and such committees and other subordinate bodies as are necessary in the judgment of the Assembly or Council to implement this Convention's objectives. The AIIP and all its component entities and functions will be funded by a mandatory assessment imposed biannually upon its Members in accordance with a formula proposed by the Council and approved by the Assembly.

1. *Assembly.* The AIIP Assembly will consist of all States Parties, each of which will be represented by an individual competent in cyber technologies, who will have a single vote on all Assembly activities. The Assembly shall meet at least once every three (3) years and shall make decisions by a majority

of Members voting. The Assembly shall have the following responsibilities and powers:

(a) to adopt objectives and policies authorized by and consistent with this Convention;

(b) to instruct the Council to formulate and/or implement measures to achieve such objectives and policies;

(c) to consider and approve standards and practices proposed by the Council for adoption by States Parties;

(d) to consider and approve the AIIP budget and assessment formula prepared and proposed by the Council;

(e) to recommend to States Parties modifications or supplementary agreements to the present Convention, including the addition of types of conduct to be considered criminal;

(f) to elect no fewer than one-fifth and no more than one-fourth of its Members to the Council, which shall include at least one representative from each of the five Permanent Members of the United Nations Security Council;

(g) to consider and approve proposals by the Council to provide technical and material assistance to deserving States Parties for the purpose of encouraging the safe and widespread use of the international information infrastructure;

(h) to propose to all States Parties as recommendations or as proposed amendments to this Convention, standards, practices, and technological measures approved by the Council;

(i) to consider and approve measures proposed by the Council to prevent any State from being used as a safe haven or otherwise in order to enable persons to secure protection from successful prevention, investigation, or prosecution for conduct set forth in Articles 3 and 4; and,

(j) to adopt regulations for its own governance, which shall include authority to suspend or expel States Parties, and to recommend to States Parties the exclusion of any State from participation in the international information infrastructure, for conduct that undermines the objectives of this Convention, on a vote of at least two-thirds (2/3) of all States Parties voting.

2. *Council.* The AIIP Council will consist of representatives from Member States elected by the Assembly. The Council shall meet at least once every

year and shall decide on all matters by majority vote. The Council shall have the following responsibilities and powers:

(a) to prepare the AIIP budget and assessment formula for consideration and approval by the Assembly;

(b) to appoint and supervise the Secretary General, and to provide for a Secretariat to administer AIIP activities with a staff limited in number and role to the extent that reliance on nonpermanent volunteer and contract personnel is practicable;

(c) to appoint standing and special committees, consisting of persons from the public and private sectors (including volunteers) who are experts in the fields of the committees' activities, which shall meet as necessary to consider and recommend to the Council standards and practices, as well as technological measures to improve the security of information infrastructures, including the capacities of States Parties and law enforcement agencies to detect, prevent, investigate, and successfully prosecute conduct set forth in Articles 3 and 4, and to prevent any State from being used as a safe haven;

(d) to consider, and where the Council sees fit to propose to the Assembly for adoption as recommendations, or as proposed amendments to this Convention, standards, practices, or measures prepared by the AIIP's standing or special committees, taking into account the work of public and private entities, such as the IETF, in order to ensure consistency of standards and practices;

(e) to receive, consider, and report to the Assembly concerning the annual reports filed by States Parties under Article 14;

(f) to consider and to recommend to the Assembly which States Parties should be deemed eligible for technical and financial assistance to enable them to satisfy their obligations under this Convention and to participate to the extent feasible in useful activities associated with cyber systems;

(g) to adopt and implement programs of technical and financial assistance to all States Parties, including training programs for law enforcement and cyber security personnel, with particular attention to reaching States Parties eligible for financial assistance, and to work with other public and private organizations in this regard;

(h) to consider and recommend as appropriate to the Assembly sanctions

on States Parties or other States for conduct that undermines the objectives of this Convention; and,

(i) to adopt regulations for its own governance.

3. *Secretariat.* The Secretariat will function as directed by the Secretary General. The Secretariat staff provided for by the Assembly, on recommendation of the Council, will be appointed by the Secretary General.

4. *Public Participation.* Meetings of the Assembly and Council of the AIIP shall be open to the public, with such public participation as is feasible. Meetings of committees, working groups, and other AIIP entities shall also be open to the public, subject to the need for confidential consideration of sensitive information.

Article 13
Protection of Privacy and Other Human Rights

1. This Convention shall not be construed to require an infringement of the privacy or other human rights of any person as defined by the laws of the State Party requested to perform any duty agreed to under this Convention. A State Party may decline to perform any duty agreed to under this Convention if it determines that doing so would be manifestly inconsistent with its established public policy.

2. As part of the obligation to establish systematic monitoring of implementation of this Convention under Article 14, a permanent subcommittee of experts shall be established by the Council to evaluate and comment upon the manner in which the Convention is being implemented with regard to the protection of privacy and other human rights, and to recommend appropriate measures to the Council and Assembly for the purpose of protecting such rights.

Article 14
Annual Reports of States Parties

1. Each State Party shall on or before the end of each calendar year commencing with the year of its accession to this Convention provide to the AIIP any relevant information concerning:

(a) the legislative and administrative measures taken by it to implement this Convention.

(b) any change in its domestic laws and regulations affecting the implementation of this Convention;

(c) the circumstances of any offense over which it has established its jurisdiction pursuant to Article 5;

(d) the measures taken by it in relation to each alleged offender who was detained for any period of time under the Convention or under its domestic law implementing all or any part of the Convention, and, in particular, the results of any extradition or other legal proceedings; and

(e) any decision not to implement a standard or recommended practice approved by the AIIP Assembly.

2. The AIIP Secretariat shall annually collate and transmit to all States Parties the information collected from them under this Article 14.

Article 15
Signature, Ratification, Acceptance, Approval, Accession, and Reservations

1. This Convention shall be open for signature by any State after _____ [DATE] at _____ [LOCATION IN DEPOSITARY STATE], in the State of _____, which shall act as Depositary.

2. This Convention is subject to ratification, acceptance, approval, or accession. The instruments of ratification, acceptance, approval, or accession shall be deposited with the Depositary State.

Article 16
Entry into Force

1. This Convention shall enter into force on the thirtieth (30th) day following the date of the deposit of the _____ [ORDINAL NUMBER] instrument of ratification, acceptance, approval, or accession with the Depositary State.

2. For each State ratifying, accepting, approving, or acceding to the Convention after the deposit of the _____ [ORDINAL NUMBER] instrument of ratification, acceptance, approval, or accession, the Convention shall enter into force on the thirtieth (30th) day after deposit by such State of its instrument of ratification, acceptance, approval, or accession with the Depositary State.

Article 17
Amendments

1. A State Party or the AIIP may propose an amendment to this Convention and file it with the Depositary State. The Depositary State shall communicate each proposed amendment to the States Parties. If, within four (4) months from the date of such communication, at least a _____ [FRACTION] majority of States Parties vote for approval of the amendment the Depositary State shall so inform all States Parties, who will thereafter communicate any ratification of such proposed amendments. Proposed amendments will become effective upon their ratification by a _____ [FRACTION] majority of States Parties.

2. When an amendment enters into force, it shall be binding on those States Parties that have ratified it. Other States Parties will remain bound by the provisions of the present Convention and any earlier amendments that they have ratified.

Article 18
Denunciation

A State Party may denounce this Convention by written notification to the Depositary State. The Depositary State shall promptly communicate the receipt of such notification to the other States Parties. Denunciation shall become effective one (1) year after the date of receipt of such notification.

Article 19
Political Offenses and Prejudicial Actions

1. None of the offenses or conduct set forth in Articles 3 and 4 shall be regarded, for the purposes of extradition or mutual legal assistance, as a political offense or as an offense equivalent to a political offense.

2. Nothing in this Convention shall be interpreted as imposing an obligation to extradite or to afford mutual legal assistance, if the requested State Party has substantial grounds for believing that the request for extradition for offenses set forth in Articles 3 and 4 or for mutual legal assistance with respect to such offenses has been made for the purpose of prosecuting or punishing a person on account of that person's race, religion, nationality, ethnic origin, or political belief.

Article 20
State Conduct

This Convention shall not apply to any state conduct undertaken for a public, noncommercial purpose, including activities undertaken by military forces of a State Party, or to a State Party's activities related to an ongoing armed conflict.

Article 21
Dispute Resolution

1. States Parties shall attempt to resolve all disputes that arise under this Convention through negotiation and mediation, with the assistance of the AIIP Secretariat.

2. Any State Party may give notice to another that it intends to seek arbitration of a specified dispute, to commence no sooner than ninety (90) days after such notice is received by the Party to whom it is sent. If the Parties are unable to agree on an arbitral tribunal or on any other necessary aspect of the requested arbitration, the matter will be referred by the requesting Party for decision under the auspices of _____ [ADD ARBITRATION MECHANISM].

3. The AIIP Council shall as soon as practicable develop and propose to the Assembly a dispute resolution mechanism that is informal, speedy, and based on appropriate expert involvement.

Article 22
Languages and Depositary

The original of this Convention, of which the English, French, and Russian texts are equally authentic, shall be deposited with the Depositary State, which shall send certified copies thereof to all States Parties.

IN WITNESS WHEREOF, the undersigned, being duly authorized thereto by their respective Governments, have signed this Convention, opened for signature at _____ [PLACE IN DEPOSITARY STATE] on _____ [DATE].

HOOVER NATIONAL SECURITY FORUM SERIES

The Transnational Dimension of Cyber Crime and Terrorism

EDITORS

Abraham D. Sofaer

Seymour E. Goodman

CONTRIBUTING AUTHORS

Mariano-Florentino Cuéllar

Ekaterina A. Drozdova

David D. Elliott

Seymour E. Goodman

Gregory D. Grove

Stephen J. Lukasik

Tonya L. Putnam

Abraham D. Sofaer

H. H. Whiteman

George D. Wilson

Hoover Institution Press Stanford University Stanford, California

The Hoover Institution on War, Revolution and Peace,
founded at Stanford University in 1919 by Herbert Hoover,
who went on to become the thirty-first president of
the United States, is an interdisciplinary research center
for advanced study on domestic and international affairs.
The views expressed in its publications are entirely those of
the authors and do not necessarily reflect the views of the staff,
officers, or Board of Overseers of the Hoover Institution.

www.hoover.org

Hoover Institution Press Publication No. 490
Copyright © 2001 by the Board of Trustees of the
Leland Stanford Junior University
All rights reserved. No part of this publication may be reproduced,
stored in a retrieval system, or transmitted in any form or by any
means, electronic, mechanical, photocopying, recording, or otherwise,
without written permission of the publisher.

First printing 2001
06 05 04 03 02 01 9 8 7 6 5 4 3 2 1

Manufactured in the United States of America
The paper used in this publication meets the minimum requirements
of American National Standard for Information Sciences—Permanence
of Paper for Printed Library Materials, ANSI Z39.48-1984. ♾

Library of Congress Cataloging-in-Publication Data
The transnational dimension of cyber crime and terrorism /
Abraham D. Sofaer, Seymour E. Goodman [editors] ;
Mariano-Florentino Cuéllar [... et al.].
p. cm. — (Hoover national security forum series)
Includes bibliographical references and index.
ISBN 0-8179-9982-5 (alk. paper)
1. Computer crimes—Congresses. 2. Cyberterrorism—
Congresses. I. Sofaer, Abraham D. II. Goodman, Seymour E.
III. Cuéllar, Mariano-Florentino. IV. Series.
HV6773 .T7 2001
364'.47—dc21 2001024693