

**A Proposal for an International Convention on Cyber Crime and Terrorism**

**Abraham D. Sofaer  
Seymour E. Goodman**

**Mariano-Florentino Cuéllar  
Ekaterina A. Drozdova  
David D. Elliott  
Gregory D. Grove  
Stephen J. Lukasik  
Tonya L. Putnam  
George D. Wilson**

**August 2000**

**Jointly Sponsored By:**

The Hoover Institution  
The Consortium for Research on Information Security and Policy (CRISP)  
The Center for International Security and Cooperation (CISAC)

Stanford University

The opinions expressed here are those of the authors and do not necessarily represent the positions of the Hoover Institution, CISAC, CRISP, their supporters, the U.S. Government (or any department or agency thereof) or Stanford University.

## **Executive Summary**

The information infrastructure is increasingly under attack by cyber criminals. The number, cost, and sophistication of attacks are increasing at alarming rates. Worldwide aggregate annual damage from attacks is now measured in billions of U.S. dollars. Attacks threaten the substantial and growing reliance of commerce, governments, and the public upon the information infrastructure to conduct business, carry messages, and process information. Most significant attacks are transnational by design, with victims throughout the world.

Measures thus far adopted by the private and public sectors have not provided an adequate level of security. While new methods of attack have been accurately predicted by experts and some large attacks have been detected in early stages, efforts to prevent or deter them have been largely unsuccessful, with increasingly damaging consequences. Information necessary to combat attacks has not been timely shared. Investigations have been slow and difficult to coordinate. Some attacks are from States that lack adequate laws governing deliberate destructive conduct. Such international cooperation as occurs is voluntary and inadequate. Some significant enhancement of defensive capabilities seems essential. Cyber crime is quintessentially transnational, and will often involve jurisdictional assertions of multiple States. Agreements on jurisdiction and enforcement must be developed to avoid conflicting claims.

The need and methods for effecting international cooperation in dealing with cyber crime and terrorism were the subject of a conference sponsored by the Hoover Institution, the Consortium for Research on Information Security and Policy (CRISP) and the Center for International Security and Cooperation (CISAC) at Stanford University on December 6-7, 1999 (the "Stanford Conference"). Members of government, industry, NGOs, and academia from many nations met at Stanford to discuss the growing problem. A clear consensus emerged that greater international cooperation is required, and considerable agreement that a multilateral treaty focused on criminal abuse of cyber systems would help build the necessary cooperative framework. (A synthesis of the Stanford Conference papers and discussion will be published by the Hoover Press.) This monograph summarizes and presents the Stanford Draft International Convention to Enhance Security from Cyber Crime and Terrorism (the "Stanford Draft" or the "Draft") and commentary on the Draft. The Draft acknowledges

and builds upon the draft Convention on Cyber Crime proposed by the Council of Europe (the "COE Draft").

#### Why a Multilateral Convention

- Cyber crime is transnational, and requires a transnational response.
- Cyber criminals exploit weaknesses in the laws and enforcement practices of States, exposing all other States to dangers that are beyond their capacity unilaterally or bilaterally to respond.
- The speed and technical complexity of cyber activities requires prearranged, agreed procedures for cooperation in investigating and responding to threats and attacks.
- A multilateral convention will ensure that all States Parties:
  - adopt laws making dangerous cyber activities criminal;
  - enforce those laws or extradite criminals for prosecution by other States;
  - cooperate in investigating criminal activities and in providing usable evidence for prosecutions; and
  - participate in formulating and agree to adopt and implement standards and practices that enhance safety and security.
- An international agency created pursuant to the draft Convention will provide a forum for international discussion, ongoing response to technological developments, and technical assistance to developing States.

### *Offenses Defined*

The Stanford Draft is designed to encourage universal recognition of basic offenses in cyberspace and universal agreement to cooperate in investigating, extraditing, and prosecuting perpetrators. (The Draft specifically excludes State conduct, addressing only conduct by individuals or groups.) Article 3 describes the conduct it covers, including: interfering with the function of a cyber system, cyber trespass, tampering with authentication systems, interfering with data, trafficking in illegal cyber tools, using cyber systems to further offenses specified in certain other treaties and targeting critical infrastructures. States Parties would agree to punish all the forms of conduct specified. Article 3 was drafted with the goal of securing speedy agreement among nations to adopt uniform definitions of offenses and commitments, despite having different network capabilities and political interests. Offenses related to more controversial issues, including protection of intellectual property and regulation of political, ethical or religious content, are therefore omitted. Implementation of treaty offenses will be effected in domestic law of signatories in accordance with Article 2.

### *International Cooperation in Investigation and Prosecution*

Participants at the Stanford Conference debated technical, legal, policy and diplomatic concerns, and many from these disparate disciplines agreed that the most important need in the battle against cyber crime and terrorism is to develop cooperative, personal relationships among government law enforcers and technical experts around the world. Successes have flowed from existing informal networks of experts, who cooperate to resolve transborder incidents as they occur. Even greater successes could result from harmonization of laws, technical standards setting, cooperative international emergency response mechanisms, and intelligence sharing.

The Stanford Draft requires State Party cooperation in investigation through the mutual legal assistance and law enforcement provisions specified in Articles 6 and 11. States Parties are required to exchange information, assist in gathering and preserving evidence, arrest alleged offenders, prosecute or extradite them, and to implement agreed international standards dealing with security and law enforcement.

### *Jurisdiction and Extradition*

Article 5 of the Draft confirms prescriptive and enforcement jurisdiction in States where offenses are committed; where alleged offenders are citizens, reside or are present; or where the conduct of offenders has substantial effects. Priority in jurisdiction is established, resting first where the offender is physically present when the offense occurs, second where substantial harm is suffered, and third in the State of the offender's dominant nationality. Article 7 of the Draft requires all States in which an alleged offender is present either to prosecute or to extradite.

### *An International Agency*

Article 12 of the Stanford Draft proposes an international Agency for Information Infrastructure Protection (AIIP). The AIIP is intended to serve as a formal structure in which interested groups will cooperate through experts in countries around the world in developing standards and practices concerning cyber security.

The structure of AIIP representation is inspired by treaties establishing the International Civil Aviation Organization (ICAO) and the International Telecommunication Union (ITU). All States Parties are represented in the AIIP Assembly, which would adopt objectives and policies consistent with the Convention, approve standards and practices for cooperation, and approve technical assistance programs, among other responsibilities. The AIIP Council, elected by the Assembly, would, among other duties, appoint committees to study particular problems and recommend measures to the Assembly. The Draft also provides for a Secretariat to perform administrative tasks. The AIIP would build upon and supplement, not attempt to modify or substitute for, private-sector activities.

### *Privacy and Human Rights*

Article 13 of the Stanford Draft permits States Parties to set and maintain their own standards for privacy and human rights. Consular notification and other procedural protections are provided for all persons detained pursuant to the Draft. In addition, Article 13 establishes a standing committee of the AIIP to study and recommend to the Council measures to protect privacy and other human rights.

*Commentary*

A substantial commentary precedes the Draft. The commentary discusses the emerging consensus against certain, destructive cyber activities, and the advantages and drawbacks to using a multilateral approach to address this problem. The commentary explains why certain provisions are included in the Draft, and why certain issues, such as copyright infringement and speech-related content offenses, are omitted. It compares the Stanford Draft to the COE Draft, and discusses the expected role and influence of the private sector in the development of standards, and the other work of the proposed AIIP.

## **Introduction**

Methods of information infrastructure attack are neither mysterious nor difficult to foresee; at the Stanford Conference, Thomas Longstaff of the Carnegie-Mellon Computer Emergency Response Team ("CERT") predicted that, in late 1999 or early 2000, a new and very harmful distributed form of denial-of-service attack would become prevalent. He based his predictions on observations of public hacker exchanges that shared attack strategies and software to implement those strategies. Longstaff predicted precisely the method that was used by hackers in the subsequent, worldwide, February 2000 attacks on CNN, eBay, Yahoo!, Amazon.com, online investment firms and others. Despite being able to anticipate attacks of this type, law enforcement personnel were unable to prevent them, and security personal employed by the targeted cyber systems were unable to defend against them. These troubling failures stem from serious weaknesses in the capacities of states to protect valuable cyber systems from attacks that pose a rapidly escalating danger. As Longstaff stated, effective methods to protect against distributed denial of service attacks may be best addressed by regional, national and international cooperation.

The open and defiant manner in which attackers currently operate reflects the weakness of the legal, defensive, and investigative capacities of the current system. Some attackers are snared after long, expensive investigations, but most go unpunished. The incapacities stem ultimately from the fact that the information infrastructure is transnational in nature. Attackers deliberately fashion their efforts to exploit the absence of internationally agreed standards of behavior and cooperation. For example, attackers can avoid prosecution or greatly complicate investigations simply by initiating attack packets from countries with inadequate laws, and routing them through countries that with different laws and practices, and no structures for cooperation.

The lack of an adequate international response to these weaknesses is puzzling, given the huge and growing financial impact of cyber attacks and crimes. Even if some estimates of damages are inflated, the problem has grown undeniably expensive to businesses, governments, and individual users around the world. Multilateral action is required to build security into the underlying technical and social architecture. History has shown that when nations agree upon a common malicious threat, be it piracy on the

high seas centuries ago or aviation terrorism of the 20th century, a cooperative, treaty-mediated regime can contribute substantially in addressing the problem.

The challenge of controlling cyber crime in its most critical dimensions requires a full range of responses, including both voluntary and legally-mandated cooperation. A consensus exists concerning many forms of conduct that should be treated as cyber crime. Common positions are developing or can be crafted to facilitate cooperation in investigation, the preservation of evidence, and extradition. Cooperation is also essential in the development and implementation of technological solutions and standards to enhance the capacity of states and users effectively to protect computers and systems from future attacks.

The nature and culture of the cyber world demand that these responses be fashioned to maximize private-sector participation and control, as well as to ensure that privacy and other human rights are not adversely affected. Certain elements of an effective program against cyber crime will require state control or approval, however. In addition, to develop and secure the universal adoption of technological and policy standards to defend against, prosecute, and deter cyber crime and terrorism will require an international forum with the necessary authority and capacities. This can be achieved by creating an international Agency for Information Infrastructure Protection (AIIP), an agency designed to reflect the particular needs and nature of the largely self-regulated cyber world and modeled after the International Civil Aviation Organization (ICAO) and the International Telecommunication Union (ITU).

While recent growth and reliance on the information infrastructures has occurred in the absence of substantial government involvement, the notion that voluntary activities alone can create adequate security for cyber activities that now involve 300 million people on the Internet alone is simply untenable. At the national level, cyber crime would likely be even more prevalent and costly than it has been had governments left the area unpoliced. The laws thus far adopted that make cyber attacks criminal have at least provided a vehicle by which to arrest – and thereby to stop, punish, and deter – cyber criminals. The great majority of users – commercial, educational, personal – favor law over anarchy when it comes to cyber attacks designed to steal, defraud, and destroy. The same is true on the international level, where only through government action can laws be passed setting universal standards for misconduct, authorizing investigatory cooperation, extradition, and the adoption of technologically-advanced methods for detecting, blocking, tracking, and deterring prohibited conduct.

Multilateral leadership must not mean the subordination of private leadership and influence over cyber technology and operations. The cyber revolution has been uniquely successful and rapid because it is led and largely controlled by the private sector. Government has, however, played a pivotal role in supporting and giving legal authority to private institutions. This distribution of power and responsibility can continue, and indeed be enhanced, by the continuing support and authority of the AIIP. Governments cannot responsibly expect the private sector to solve the cyber security problem. Business stakeholders in the information infrastructure have made clear that the private sector cannot be expected to perform the roles traditionally performed by law enforcement. But an enhanced government role need not be one that requires significantly greater domestic powers or more intrusive measures; rather, the need is for international cooperation to create common standards and practices. These objectives can be achieved without conferring inappropriate or unnecessary powers on governments to regulate and to intrude upon cyber systems, while at the same time preserving private-sector control of this uniquely productive and dynamic sector.

## **Commentary on the Draft Convention**

The case for international cooperation in dealing with cyber crime is overwhelming. The debate currently under way is over the form and scope such cooperation should take, and the extent to which the United States and other technologically advanced States should rely upon multilateral efforts to enhance cyber security.

Proposals for voluntary international cooperation have been advanced and are being implemented<sup>1</sup>. The principal elements of these proposals – to train law enforcement officials to understand and cope with cyber crimes, and to establish round-the-clock emergency response teams – are widely supported. In addition, the Group of Eight (G-8)<sup>2</sup> and private groups such as the Internet Alliance<sup>3</sup> have issued guidelines aimed at making voluntary cooperation more effective. While these groups recognize that international cooperation is essential, they have yet to accept the idea that an international treaty should be negotiated establishing legally-mandated standards and obligations.

Support for voluntary, as opposed to legally-mandated, international measures rests upon several arguments. Most cyber crime, it is argued, is conventional crime (e.g., fraud, drug dealing, money laundering, sexual exploitation of minors), in which cyber technology happens to be used. Existing treaties and international arrangements, including those providing for extradition and legal assistance, are potentially applicable

---

<sup>1</sup> See, e.g., Remarks of Attorney General Janet Reno to the National Association of Attorneys General (Jan. 10, 2000), available at <<http://www.usdoj.gov/ag/speeches/>>; U.S. Department of Justice Computer Crime and Intellectual Property Section (CCIPS) materials, including "The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet: A Report of the President's Working Group on Unlawful Conduct on the Internet" (Mar. 2000), available at <<http://www.usdoj.gov/criminal/cybercrime/>>.

<sup>2</sup> See, e.g., "Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime" (Moscow, Oct. 19-20, 1999), Communiqué, available at <<http://www.library.utoronto.ca/g7/adhoc/crime99.htm>>. See also Tom Heneghan, "G8 Nations Meet to Discuss Cybercrime" (May 15, 2000), which was reported at <[http://dailynews.yahoo.com/h/nm/20000515/ts/crime\\_cyberspace\\_2.html](http://dailynews.yahoo.com/h/nm/20000515/ts/crime_cyberspace_2.html)>.

<sup>3</sup> See the materials posted at <<http://www.Internetalliance.org/policy/index.html>>, as well as "Testimony of Jeff B. Richards, Executive Director of the Internet Alliance, Before the U.S. Senate Committee on Appropriations, Subcommittee on Commerce, Justice, State, and Judiciary," *Hearing on Cybercrime* (Feb. 16, 2000), available at <[http://www.senate.gov/~appropriations/commerce/richards\\_00.html](http://www.senate.gov/~appropriations/commerce/richards_00.html)>.

in these cases. Securing international agreement on the wording of new cyber crimes will be difficult, moreover, and vast differences exist among States regarding appropriate regulation of content, the proper scope of transnational investigation, and the bases upon which tracking information and messages should be subject to seizure and scrutiny. Furthermore, a great disparity exists among States – even technologically advanced ones – as to the scope of privacy and other rights possessed by individuals under national laws that would either operate to limit an international agreement or be compromised by one. Finally, the Internet, many believe, has been a powerful vehicle for economic growth and enhanced communication in large part because it is controlled by the private sector, rather than governments; and this growth and creativity may be adversely affected by international legal requirements and regulation.

For these reasons, Drew C. Arena, then Senior Counsel to the Assistant Attorney General, U.S. Department of Justice, commented at the Stanford Conference that achieving consensus on "the specific steps" to be taken in negotiating a multilateral treaty would be "too hard" at the present time to warrant the effort.<sup>4</sup> University of Chicago School of Law Professor Jack L. Goldsmith has argued that, in the absence of a suitable international regime, the United States should rely on unilateral measures in fighting transnational cyber crime.<sup>5</sup> However, he does, in principle, favor the pursuit of such a regime.

These arguments against the creation of an international legal regime to deal with cyber security are cogent, but based on difficulties and dangers that are avoidable. The case for a multilateral agreement to combat cyber crime and terrorism is strong, and the need to undertake the effort of negotiating one is becoming clearer with the increasing costs of such activity. While it may be true that most crimes in which computers and networks are involved are conventional and potentially covered by international agreements, these are not the crimes against which a new treaty is needed. Existing international agreements provide no help in dealing with crimes related directly to the

---

<sup>4</sup> Drew C. Arena, "Obstacles to Consensus in Multilateral Responses to Cyber Crime." Presentation at the Conference on International Cooperation to Combat Cyber Crime and Terrorism, Hoover Institution, Stanford University, Stanford, California (Dec. 6-7, 1999), p. 3.

<sup>5</sup> Jack L. Goldsmith, "Cybercrime and Jurisdiction." Presentation at the Conference on International Cooperation to Combat Cyber Crime and Terrorism, Hoover Institution, Stanford University, Stanford, California (Dec. 6-7, 1999), p. 9.

information infrastructure, including attacks utilizing viruses (such as "Melissa" and "I Love You"), denials of service, and other destructive conduct. Furthermore, the need for an international agreement to deal with cyber crime rests not merely on the fact that such acts include new types of conduct but also on the need for new methods by which cyber crimes will have to be investigated and prosecuted to provide effective protection. To secure multilateral agreement on the precise wording of cyber crimes would, in fact, be complicated; but that effort need not be undertaken. A broad consensus exists with regard to certain conduct involving the information infrastructure that should be made criminal;<sup>6</sup> and a treaty could readily be drafted that describes such conduct and requires all States Parties to make such conduct criminal through any formula they choose to utilize.

The differences that exist among States concerning several key issues in developing a treaty must be taken into account and will limit and shape the arrangements that are currently feasible. But differences concerning such issues as regulation of content, scope of extraterritorial investigation, standards of proof, and protection of privacy and other rights, can be resolved, largely through a willingness to begin this effort by focusing on measures likely to secure universal agreement. The sharp differences that exist among States with regard to what can be done unilaterally demonstrate, in fact, the need to attempt to secure agreed, multilateral arrangements, rather than establishing a basis for making no effort to do so.

The notion that the United States should act unilaterally when necessary to protect its interests is in principle sound. Professor Goldsmith seems to recognize, however, that unilateral activities must be legally defensible, and resort to them must be in the nation's best interests. His assumption that it will take many years to negotiate and implement a multilateral convention may turn out to be wrong, in light of the increasingly obvious need and growing momentum for such an arrangement. Furthermore, even before a multilateral treaty is complete, the United States may be able to reach less comprehensive arrangements with other States to enhance legal protections. Unilateral conduct that offends other States, and leads them to reject or delay negotiating a desirable treaty, would harm U.S. interests.

---

<sup>6</sup> See Tonya L. Putnam & David D. Elliott, "International Responses to Cyber Crime," Chapter 2, *International Cooperation to Combat Cyber Crime and Terrorism* (forthcoming, Hoover Press).

Concerns expressed by the private sector over establishing legally-mandated norms and obligations stem from the fear that law enforcement considerations will adversely affect (and greatly burden) Internet businesses and freedom of expression. Government control of the information infrastructure could well have detrimental effects, and international regulation could be especially damaging if political objectives and bureaucratic requirements are allowed to interfere with the present, privately dominated Internet regime.<sup>7</sup> National governments – including the U.S. government – have sought or imposed potentially damaging restrictions on Internet users, including limitations on the use and sale of advanced encryption, demands for the power to intrude upon, hear, and record Internet traffic,<sup>8</sup> and suggestions that private entities assume quasi-prosecutorial responsibilities in criminal investigations. These policies and suggestions have, however, unjustifiably evoked suspicion of all efforts to establish legally-mandated obligations. If, as we believe, voluntary efforts will not provide adequate security, legal obligations to cooperate can be devised that are consistent with continued private creativity and control. An international regime can be fashioned to satisfy the full range of cyber-security needs, in a manner that ensures continued private-sector control of Internet technology and practices. The United States is party to several international regimes encompassing the creation of consensus-based, non-mandatory measures crafted by public and private-sector experts, on which a treaty for cyber security could draw in providing a comprehensive and lasting system for international cooperation.

The strong case for a legally-mandated, international regime has led to several significant developments. Treaty provisions are being proposed to close loopholes in existing multilateral commitments in the specific area of civil aviation.<sup>9</sup> This approach

---

<sup>7</sup> See Stephen J. Lukasik, "Current and Future Technical Capabilities," Chapter 4, *International Cooperation to Combat Cyber Crime and Terrorism* (forthcoming, Hoover Press), for a description of the present governing structure of the Internet.

<sup>8</sup> Consider, for example, the Clinton Administration's January 2000 "National Plan for Information Systems Protection," which drew criticism for, among other things, relying too heavily on monitoring and surveillance instead of simply focusing on making systems more secure. See "Jennifer Jones, "U.S. Cyberattack Protection Plan Draws Criticism" (Feb. 3, 2000), which was reported at <<http://cnn.com/2000/TEC...cyberprotection.crit.idg/index.html>>.

<sup>9</sup> See Mariano-Florentino Cuéllar, "Past as Prologue: International Aviation Security Treaties as Precedents for International Cooperation against Cyber Terrorism and Cyber Crimes," Chapter 3, *International Cooperation to Combat Cyber Crime and Terrorism* (forthcoming, Hoover Press).

may be feasible in other areas, particularly to protect critical infrastructures from criminal and terrorist attacks, and seems likely to cause little controversy.

The Council of Europe (COE) has adopted a more comprehensive approach, recently publishing a draft treaty on cyber crime.<sup>10</sup> This proposal includes definitions of cyber activities that must be made criminal by all States Parties, as well as other features and forms of cooperation.<sup>11</sup> The COE's draft assumes, correctly, that substantial consensus exists with respect to those cyber activities that should be considered criminal, and that substantial benefits can be derived from a multilateral arrangement with common standards, investigative cooperation, and extradition.

We undertake in this monograph to demonstrate the advantages and feasibility of an even more comprehensive regime by proposing a draft international convention (the Stanford Draft) and discussing its principal elements. The Stanford Draft is largely consistent with the draft COE Convention on Cyber-Crime, but differs in some respects. Most significantly, the Stanford Draft would establish an international agency, modeled along the lines of successful, specialized United Nations agencies, to prepare and promulgate – on the basis of advice from non-political experts – standards and recommended practices (SARPs) to enhance the effectiveness of protective and investigative measures.

1. Covered Conduct. The basis for international cooperation rests, most fundamentally, on the combination of a demonstrable need for international agreement to combat harmful cyber conduct, and the existence of an international consensus on what conduct should be considered criminal. A review of existing statutory law and proposed international arrangements reflects widespread consensus on prosecuting as criminal the conduct covered in the Stanford Draft: attacks aimed at disrupting or damaging computer operations; deliberate and unauthorized intrusions; interference with computer-security measures; maliciously altering content; intentionally and materially facilitating the

---

<sup>10</sup> See "Draft Convention on Cyber-Crime," released for public discussion on April 27, 2000, available at <<http://conventions.coe.int/treaty/en/projets/cybercrime.htm>>. The COE's Justice Ministers resolved on June 9, 2000 that the Council should speed its work and "conclude an international treaty by the end of the year." See <[http://www.coe.fr/cp/2000/427a\(2000\).htm](http://www.coe.fr/cp/2000/427a(2000).htm)>.

<sup>11</sup> See, e.g., id., ch. II ("Measures to be taken at the national level"), §§ 1-3 ("Substantive criminal law," "Procedural law," and "Jurisdiction"). See also id., ch. III ("International Co-operation").

commission of prohibited conduct; using a cyber system in committing violations of any of several widely-adopted antiterrorist conventions; and using a cyber system to attack critical infrastructures. Most of these forms of conduct are covered in the COE's draft proposal, although that draft attempts to categorize cyber crimes into a number of specific categories: illegal access;<sup>12</sup> illegal interception; data interference; system interference; and the possession or transfer of "illegal devices" under specified circumstances. The COE effort to generalize may have created coverage on some issues that is undesirably broad.<sup>13</sup> The introductory language to Article 3 of the Draft – specifically the concept of "legally recognized authority" – is intended to incorporate the concept of self-defense. Efforts of governments, companies, and individuals to defend themselves from attacks may sometimes require measures which, if adopted without authorization or justification, would be criminal, such as alterations of code, or interfering with operation of computers being used by attackers. At times, such efforts may affect innocent third parties, but nonetheless may be reasonable. The complex issues that are certain to arise in applying established principles of law to this new area of technological activity will be resolved over time, on the basis of experience.<sup>14</sup>

The Stanford Draft recognizes and attempts to deal with the fact that States have dissimilar standards in statutes that cover the conduct it proscribes. Instead of attempting to list specific, commonly defined "offenses," as in most extradition treaties, the Stanford Draft refers to types of conduct, and secures commitments from all States Party to enforce any applicable law against every form of covered conduct, or to adopt new

---

<sup>12</sup> See "Draft Convention on Cyber-Crime," *supra* n. 10, available at <<http://conventions.coe.int/treaty/en/projets/cybercrime.htm>>, arts. 2-6. The prohibition on illegal access would prohibit intentional access to any part of a computer system "without right." It then continues: "A party may require that the offence be committed either by infringing security measures or with the intent of obtaining computer data or other dishonest intent." To the extent the COE Draft permits Members to vary the conduct covered by the treaty, in this and some other provisions, the treaty's effectiveness will be undermined. Uniformity of commitments is in general of greater importance than any particular form or level of coverage.

<sup>13</sup> The definition of illegal interception, for example, might be read to include interceptions, albeit without right, of data that no effort has been made to protect. *See id.*, art. 3.

<sup>14</sup> *See generally* Gregory D. Grove, Seymour E. Goodman, Stephen J. Lukasik, "Cyber-attacks, Counter-attacks and International Law," 42 *Survival* (forthcoming: IISS, London, Autumn 2000).

laws necessary to create authority to prosecute or extradite for such conduct. This approach overcomes the problem of attempting to develop precise, agreed definitions of offenses, and therefore the requirement that every State Party adopt particular formulations as national crimes.

In addition to requiring criminal enforcement against conduct specifically aimed at the information infrastructure, the Stanford Draft requires criminal enforcement against the use of computers in the commission of offenses under certain, widely-adopted multilateral treaties. These include clearly-defined crimes against aircraft, ships, diplomats, and terrorist bombings. Computers can greatly enhance the potential damage caused by crimes, and can make them especially difficult to investigate. Therefore, since most States are parties to these multilateral treaties, they should be prepared to impose more stringent punishment for the use of cyber capacities in committing the targeted offenses. (The COE Draft currently does not include such provisions.) Other, widely recognized forms of criminal conduct may also become more aggravated through the use of computers, such as forgery, fraud, theft, and conversion. These crimes are not included in the Stanford Draft, however, since they are in general already encompassed in extradition treaties, to the extent States Parties want such coverage. The cyber dimension of such activities, moreover, would generally involve conduct covered in the Stanford Draft, irrespective of the crimes such conduct may have facilitated. (The COE Draft includes coverage of "computer-related" forgery and fraud, but its definitions of these offenses seem likely to cause uncertainties.<sup>15</sup>)

Other types of conduct, when related to the information infrastructure, have been prohibited in some States, including copyright violations, and sexual exploitation of minors. These offenses are covered by the COE Draft, along with the use of computers to commit fraud.<sup>16</sup> These types of conduct are not covered in the Stanford Draft because their inclusion may prove controversial. In fact, a sufficient consensus for including some of these offenses – especially the use of computers for sexual exploitation of minors – may exist; the Stanford Draft's coverage could be expanded to include such offenses. (The COE Draft covers offenses related to child pornography, as well as "copyright and related

---

<sup>15</sup> The definition of forgery, for example, leaves Members free to require or dispense with any dishonest intent, and that of fraud requires neither a false representation nor reliance. *See id.*, arts. 7 & 8.

<sup>16</sup> *See id.*, art. 8.

offences," but whether the scope of coverage should be coterminous with treaties in the area – such as the Berne Convention and other copyright treaties administered by the World Intellectual Property Organization – has been left unsettled.<sup>17)</sup>

The Stanford Draft also includes very limited coverage of "content" offenses, to avoid the strong differences that exist among States concerning restrictions on speech and political activity. No type of speech, or publication, is required to be treated as criminal under the Stanford Draft; if, for example, Germany were to decide to ban publication on the Internet of *Mein Kampf*, it would have to do so unilaterally and could not expect to receive enforcement assistance under the Stanford Draft. The single exception to this principle in the Stanford Draft is the narrow coverage of conduct described as the "distribution of devices or programs intended for the purpose of committing" other conduct made criminal by the Stanford Draft. The Draft thereby makes criminal the knowing and deliberate effort to cause illegal attacks through such distribution, but not discussions of computer vulnerability intended for evaluating exposure to attacks on the Internet, or other protected speech. States Parties wishing to encourage open discussion of computer attacks and vulnerabilities could designate "safe harbor" sites at which discussion would be considered lawful. (The COE Draft would prohibit a broad range of conduct involving the transfer or possession of "illegal devices," defined to include certain computer programs.<sup>18)</sup>)

A final issue concerning offenses is whether a cyber-crime convention should cover only those offenses that provide for penalties exceeding some minimum term of imprisonment. Extradition treaties generally contain such a limitation, usually that the crime for which extradition is sought be punishable by one year of imprisonment or more. This rule is intended to exclude minor offenses from coverage. Given the complications and effort required to satisfy extradition requests, this consideration is at least as important in a cyber-crime convention as in any other. By having such a requirement, moreover, States Parties would in effect be required to cover prohibited conduct with potential penalties of at least one year in prison. The Stanford Draft therefore includes only crimes for which a potential penalty of at least one year's

---

<sup>17</sup> See id., art. 10.

<sup>18</sup> See id., art. 6.

imprisonment is provided. (The COE Draft includes a separate article on this subject, which is designed to ensure serious penal and civil sanctions.<sup>19</sup>)

2. Jurisdiction. The Stanford Draft anticipates that the conduct it covers will have effects potentially conferring jurisdiction on multiple States Parties for the same offense. It provides a set of priorities that Parties would agree to follow in performing their duties and pursuing their rights, to the extent practicable, given the difficulty of anticipating all the possible contingencies. A State Party must establish jurisdiction to try offenders who commit offenses in its territory, who are its nationals, or who are stateless residents in its territory and whose extradition from its territory is refused. A State Party may establish jurisdiction to try offenders who attempt to harm it or its nationals, or to compel it to perform or abstain from performing an act, or whose offenses have substantial effects within its territory. (The COE Draft provides similar coverage, but fails to resolve aspects of this problem in a definitive manner.<sup>20</sup>)

The problem of multiple-State jurisdiction over crime is by now commonplace in international law. Transnational fraud, for example, has led to decisions by national courts assuming jurisdiction on the basis of any significant connection to the conduct involved. Among these are the States where a fraud was planned, where an effort to defraud was initiated, where individuals worked at implementing the fraud, where or through which communications were made that were intrinsic to the fraud, where the victims were located, and where the fraud had material and intended effects.<sup>21</sup> The widespread recognition of fraud as criminal activity leads States readily to find jurisdiction over such activity, despite the significant relationship particular frauds may have to other States. They tend to assume that punishing fraud will be supported by other affected States, rather than opposed as violating their sovereignty.

---

<sup>19</sup> See id., art. 13.

<sup>20</sup> See id., art. 19.

<sup>21</sup> See *Libman v. The Queen* [1985] 2 S.C.R. 178 (a leading decision of the Canadian Supreme Court providing in-depth description of modern developments with regard to jurisdiction to prosecute conduct involving extraterritorial elements). See also Laurent Belsie, "Cops Narrow Gap on Web Criminals: This Week's Arrest of a Teen Hacker Shows that Law Enforcement is Getting More Savvy," *Christian Science Monitor* (Apr. 21, 2000), available at 2000 WL 4427576 (reporting on the arrest in Montreal after investigations by the Royal Canadian Mounted Police and the FBI of "Mafiaboy" for allegedly sabotaging the CNN.com website in February 2000).

Cyber crime is quintessentially transnational, and will often involve jurisdictional assertions of multiple States. To avoid the conflict such assertions of jurisdiction could cause, enforcement under the Stanford Draft is limited to cyber activities that are universally condemned. 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. It seems likely, therefore, that States will in general accept all of the reasonably-based jurisdictional claims approved in the Draft.

3. Cooperation in Criminal Enforcement. The Stanford Draft includes commitments by States Parties to engage in the full range of cooperative activities found in widely adopted international agreements. Under it, States Parties would agree to extradite or prosecute persons reasonably believed to have engaged in any form of the covered conduct or offenses. Where necessary, and on a proper evidentiary basis, they would arrest and hold alleged offenders for a short period pending an extradition request. They would also agree to cooperate in seizing, preserving, developing, and providing in usable form evidence for the prosecution of offenders in the courts of other States Parties. They would coordinate these activities through designated "Central Authorities," as in Mutual Legal Assistance Treaties, so that each State Party would know to whom to address requests, and would have an identified agency or person responsible for dealing with such requests in a timely and proper manner.

The COE Draft is particularly impressive in mandating prompt responses to cyber attacks and requests for cooperation, on a 24-hour/7-day-per-week basis,<sup>22</sup> and the Stanford Draft incorporates a similar commitment. The COE Draft also provides detailed rules concerning seizure of data, production orders, expedited presentation, and disclosure.<sup>23</sup> A provision (Article 28) regarding "interception" is contemplated but under discussion. These rules are currently useful, but may become problematic with the availability of new technologies or methods. The Stanford Draft, for this reason, provides a commitment to cooperate on each of these subjects that is not further specified.

---

<sup>22</sup> See "Draft Convention on Cyber-Crime," *supra* n. 10, available at <<http://conventions.coe.int/treaty/en/projets/cybercrime.htm>>, arts. 29.

<sup>23</sup> See id., arts. 14-17.

The basic principles of cooperation are clear. When it comes to implementation, however, many problems exist, and many more are certain to arise, for which answers have not as yet been developed. What, for example, should be the scope of a State's power unilaterally to seek information in a foreign State? A State may not know whether its electronic effort to obtain information about a crime will enter or have any significant effect within another State or States; it could not avoid such uncertainty even if it tried. Some tolerance of extraterritorial effects would seem, therefore, to be imperative in any viable, multilateral cyber-related arrangement. Both the Stanford Draft and the COE Draft call for the widest possible cooperation; the former's provision for unilateral action is more narrowly drawn in some respects, but the latter's is still not agreed upon by COE Members.<sup>24</sup>

Another area of current uncertainty is what duties an Internet Service Provider (ISP) should have to preserve and provide information of cyber crimes. Should any such duty be enforceable by law, moreover, and if so by what means? These are sensitive issues, since States have not yet imposed duties on ISPs and other Internet participants, such as those imposed in analogous contexts. What should States be required to do to enhance the prospects of preserving evidence that could be helpful in investigating an attack; in particular, should a State be required to seize such information?

These sorts of issues related to transnational investigation of cyber crime and terrorism raise several questions. The first concerns technology: what technological measures are possible and/or desirable to assist States Parties in securing cooperation that goes beyond the conventional steps currently undertaken in treaties of extradition and mutual legal assistance? Rapidly changing technological capacities and needs make it fruitless to attempt to deal definitively in a draft convention with this aspect of the cyber crime and terrorism problem.<sup>25</sup> Instead, the Draft proposes general principles supporting certain existing technological objectives, and would establish an international agency through which States Parties would cooperate in considering and proposing the use of particular technological measures to enhance cooperative efforts.

In addition to the technological dimension are certain questions of principle concerning the right of States Parties to defend against or to investigate cyber crime. May

---

<sup>24</sup> Compare Article 6(5) of the Stanford Draft, *infra*, with Article 27 of the COE Draft.

<sup>25</sup> Drew Arena is correct in making this point, but wrong to assume that any multilateral regime must share this deficiency. See n. 4, *supra*, p. 10.

a State Party, for instance, deliberately initiate investigative actions or countermeasures for law-enforcement purposes that could involve sending transmissions into cyber systems located in other, sovereign territories? Based on experience to date, fast-spreading computer viruses and other cyber attacks demand prompt efforts to track down attackers, and it is difficult if not impossible to know in advance all the places to or through which any part of any cyber transmission might travel. Therefore, the Stanford Draft approves in principle unilateral measures where they are electronic and reasonable. The Stanford Draft provides, moreover, that any law enforcement activity undertaken that knowingly affects another State Party, including any effort to seek cooperative measures from an entity located in another State Party, must be made known to the Central Authority of that State as soon as practicable. In addition, the Stanford Draft would require all entities, including ISPs, to comply with any standard or procedure developed by the AIIP under the Stanford Draft and accepted by the State Party in which they are located, and would mandate that all States Parties enforce all such standards and procedures. Arrangements based on these principles seem likely to garner widespread support, and would be preferable to unilateral actions that some States could find objectionable (or even criminal).

The Stanford Draft includes a provision authorizing the seizure and forfeiture of equipment utilized in the commission of offences, subject to due process protections. States could use the information contained in such equipment, or dispose of the equipment as they see fit, consistent with national law. Funds derived from forfeitures have provided resources in other areas for use in upgrading law-enforcement capabilities.<sup>26</sup> The seizure and/or forfeiture of cyber equipment used in committing covered offenses is consistent with the universally-recognized right of governments to seize instruments of crime.

4. Structure for Technological Cooperation. An effective transnational response to cyber crime requires a high level of technological cooperation with regard to virtually every function expected to be performed by the States Parties. Cyber criminals exploit the technological possibilities available, including the ability to mask their identity, to hide the origin of attacks and other actions by conducting them through intermediate

---

<sup>26</sup> See, e.g., United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Dec. 20, 1988), T.I.A.S., 20 I.L.M. 493 ("Narcotics Convention" or "Vienna Convention on Narcotics").

sites, and to find and exploit weaknesses throughout the worldwide information infrastructure. The challenges of dealing with these capacities are exacerbated, moreover, by dynamic changes in technology, the continuing development of new methods for committing cyber crimes, the current widespread sharing of information and ideas about cyber system vulnerabilities, and a culture among users of cyberspace that is skeptical of, if not outright hostile to, government involvement.

Given this context, it is unrealistic to expect that cyber crime will be significantly controlled or deterred through unilateral or voluntary or purely defensive measures. Defensive measures always make sense, and will prove effective for some entities, some of the time. But the pressure to operate openly in business, education, research, entertainment, and personal activities leads users to develop or choose accessible (and hence more vulnerable) technology. Governments have seemed especially unable to defend their sites and systems, and have been frequent targets of attack.<sup>27</sup> Furthermore, the objectives sought through cooperation, and simply unavailable to States acting unilaterally, require a high level of technological coordination.<sup>28</sup> Take, for example, the need to anticipate, freeze, and trace information packets that are used in cyber crime. Those measures, once devised, will need to be approved and implemented by all participants in the information infrastructure, in a technologically-compatible manner, or criminals will find and use gaps in coverage. Similarly, to enable States to conduct searches and seizures, to provide for extradition, and to develop evidence that is usable in the courts of all cooperating States, will require adoption of uniform and mutually acceptable standards and technological solutions, on which all States can rely.

---

<sup>27</sup> Consider, for example, the numerous attacks in January 2000 that paralyzed several Japanese government websites. See Howard W. French, "Internet Raiders in Japan Denounce Rape of Nanjing," *New York Times* (Jan. 31, 2000), available at 2000 WL 12395311 (reporting that hackers posted messages on the website of Japan's postal service criticizing Japan's wartime role in China in the 1930s, "as a series of similar attacks" over the previous week "began to look like a daily ritual"). See also "Hackers Become an Increasing Threat," *New York Times* on the Web/Breaking News from Associated Press (Jul. 7, 1999) (reporting on "high-profile electronic assaults [that] have included [U.S.] government" sites such as the White House, FBI, Senate, and Army Department), which was reported at <<http://www.nytimes.com/aponline/w/AP-Hacker-Threat.html>>. And see Daniel Verton, "Cyberattacks Against DOD up 300 Percent This Year," which was reported at *CNN.com* (Nov. 5, 1999).

<sup>28</sup> Recall the discussion by Stephen Lukasik in Chapter 4, n. 7, *supra*.

The pressures for multilateral solutions to information-infrastructure problems are, in fact, likely to be so great that solutions will be developed without the formal, open, and accountable processes associated with established international institutions. The story of how private and public actors developed and secured U.S. government support for a system of domain protection illustrates both the need for and inevitability of multilateral solutions to at least some of the key issues, as well as the ad hoc and relatively undemocratic process that may occur in the absence of established, publicly accountable mechanisms.<sup>29</sup>

The process by which effective standards and practices are established for international cooperation in dealing with cyber crime and terrorism will likely be the most important aspect of any multilateral agreement. Considerable guidance can be gained in designing a structure for setting such standards from other areas in which transnational standard-setting activities occur, such as airline safety, marine safety, telecommunications, and banking. In general, standard setting and cooperation in such areas is achieved by establishing an international agency assigned clearly-articulated and widely-shared objectives, with the technical and material resources to achieve those objectives, a professional and nonpolitical staff, substantial reliance on the private sector (especially on highly-skilled technical experts), and continuous political involvement and ultimate control by representatives of the participating States.

The history and structure of the International Civil Aviation Organization (ICAO)<sup>30</sup> are instructive in this regard.<sup>31</sup> ICAO is governed by an Assembly, consisting of representatives from all its States Parties (185), which meets at least once every three years, establishes basic policies consistent with governing treaties, considers and recommends treaty revisions, approves the budget, which it funds through an apportionment among Member States, and elects delegates to the Council for three-year

---

<sup>29</sup> See generally Yochai Benkler, "Internet Law: A Case Study in the Problem of Unilaterism," *N.Y.U. School of Law: Pub. L. & Legal Theory Working Paper Series* No. 11 (Fall 1999) (to be published in EUR. J. INT'L L., 2000) available at <[http://papers.ssrn.com/paper.taf?abstract\\_id=206828](http://papers.ssrn.com/paper.taf?abstract_id=206828)>.

<sup>30</sup> ICAO was established under Part II of the Convention on International Civil Aviation (Dec. 7, 1944), 59 Stat. 1693, 84 UNTS 389 ("Chicago Convention").

<sup>31</sup> See Mariano-Florentino Cuéllar, n. 9, *supra*, evaluating in Chapter 3 the utility of international agreements on civil aviation security as precedents for the regulation of cyber activities, and recommending specific modifications to existing civil aviation conventions to close certain loopholes.

terms. The Council currently has 33 members, including representatives from States of chief importance in air transport, from States that make the largest contributions to international aviation, or chosen to ensure that all major geographical areas are represented. The Council implements Assembly decisions, prepares the budget, administers ICAO's finances, appoints the Secretary General and provides a Secretariat, and is empowered to adopt Standards and Recommended Practices (SARPs), which are incorporated into the ICAO Convention through Annexes. The Council acts by majority vote in carrying out its functions, including in the adoption of SARPs, which are only adopted after exhaustive development and "technical monitoring, evaluation and backstopping."<sup>32</sup> While it may delegate authority with respect to any particular matter to a committee of its members, decisions of any such committee may be appealed to the Council by any interested contracting State.

The subjects dealt with in SARPs reflect the Council's authority to adopt measures necessary to maintain the safety and efficiency of international air transport. In performing these functions, the Council is assisted by the Air Navigation Commission, a body of fifteen persons with "suitable qualifications and experience," appointed by the Council from among nominees of Member States. This expert body is responsible for considering and recommending new or amended SARPs, establishing technical sub-groups, and ensuring that the Council collects and disseminates to all Member States the information necessary and useful for the advancement of air navigation.

Technical assistance is a major aspect of ICAO's work. Member States license pilots in accordance with ICAO standards. Standardization of equipment and procedures is a major aim and activity, on the whole array of technical issues, including navigation, meteorology, charts, measurement, aircraft operation, air traffic services, search and rescue, accident inquiry, and security. Developing countries are actively assisted through a variety of programs, funded by ICAO, the United Nations Development Program (UNDP), and other sources. Some 80 staff members are involved in about 120 assistance projects each year, with an overall budget of \$55 million. They provide training, technical advice, and help in purchasing necessary equipment.

---

<sup>32</sup> See "ICAO Technical Co-operation," available at <[http://www.icao.int/icao/en/tcb\\_desc.htm](http://www.icao.int/icao/en/tcb_desc.htm)>, and discussed in Chapter 3, *supra*.

A second international agency that performs duties analogous to those relevant to cyber security is the International Telecommunication Union (ITU). The ITU is the oldest intergovernmental organization in existence, having been formed in 1865 to implement the Telegraph Convention. It expanded its activities to radio in 1906, and currently deals with issues related to all forms of "telecommunications," including telephone, television, and telex. It operates along the same lines as ICAO,<sup>33</sup> with heavy reliance on private-sector expertise and involvement.<sup>34</sup> In recent statements, the ITU has expressed its intent to become more involved with information-infrastructure issues.<sup>35</sup>

The ICAO and ITU regimes deal with underlying technological matters that differ from each other, and from Internet communications, in significant ways. But the needs that led to the creation of these, and of other, similar regulatory mechanisms, are largely analogous to those affecting the cyber world. The key factors behind

---

<sup>33</sup> The ITU Plenipotentiary Conference (of about 170 members) establishes general policies consistent with governing treaties; proposes revisions to the International Telecommunication Convention when necessary; develops the basis for a budget; and elects an Administrative Council, composed of 43 members chosen with due regard to equitable geographic representation, which meets once each year, supervises the Union's administrative operations, coordinates the activities of its permanent bodies, approves the annual budget, and interacts with other international bodies. Expenses are borne by the Member States, which are divided into several contribution classes based on relevant capacities. The Plenipotentiary also elects a Secretary General, who supervises the operations of the Secretariat, which is responsible for the ITU's administrative and financial affairs. The ITU, like ICAO, has a substantial program of technical assistance and training, especially for needy States, funded in part by the UNDP.

<sup>34</sup> Technical activities constitute the bulk of the ITU's activities. It has several boards and committees of politically independent experts who make recommendations concerning technical and operating issues in different areas of telecommunications, including the International Frequency Registration Board, five radio experts elected by the Plenipotentiary from different regions of the world, which records frequency assignments and advises Member States concerning such issues as interference. In addition to representatives of Member States, experts from private companies operating telecommunication services routinely participate in the Committees' work.

<sup>35</sup> See, e.g., "ITU Efforts to Build a New Global Information Infrastructure," available through <<http://www.itu.int/newsroom/index.html>> (stating in part: "While many countries are already beginning to implement their own strategies to put in place new high-speed information infrastructures, there remains a need for a global approach which will foster worldwide compatibility between new technologies. The ITU, with its 188 government members and around 500 members from private industry, represents a global forum through which global standards that reflect the needs of a broad cross section of the infocommunications industry, from operators and governments to service providers and consumers, can be developed....").

establishment of these multilateral bodies have been safety and efficiency – the same considerations supporting a multilateral solution to the problem of cyber crime and terrorism. In addition, these multilateral entities are designed to: (1) enable all States Parties to learn of and become involved in the multilateral solutions of problems related to transnational technologies; (2) enable technologically-advanced States to protect their interests; (3) ensure that solutions are based on the best possible scientific knowledge, developed with the input of expert advice; and (4) benefit from involvement and expertise of private interests (both commercial and non-profit).

The Stanford Draft draws on the ICAO and ITU patterns in creating a proposed international institution, the "Agency for Information Infrastructure Protection" or "AIIP," to implement the objectives of States Parties with regard to protecting the information infrastructure from criminal and terrorist cyber activities. No single set of technical fixes will solve the problems that now exist, let alone those that will develop as the technological possibilities expand. The AIIP is therefore designed to play an ongoing role in formulating and revising standards, and proposing treaty revisions for enhanced safety, efficiency, and effective cooperation in light of continuing technological and political developments. Properly designed and structured, this type of agency should contribute materially to cyber security.

The Stanford Draft would require States Parties to establish the AIIP, with the following, key components: an Assembly having functions similar to those exercised by the plenary bodies that operate in ICAO, the ITU, and some other specialized agencies; a Council that implements the policies set by the Assembly, through committees of experts, with heavy private-sector representation; and a Secretary General and Secretariat to implement Assembly and Council instructions and perform administrative tasks. The Council would formulate and the Assembly would adopt recommended standards and practices (SARPs) to advance the purposes of the Stanford Draft, and the AIIP would also propose amendments and additional international agreements to implement solutions to problems that require new authority from States. Some of the UN's specialized agencies have an impressive record for developing and proposing international agreements to deal with important areas not covered by their founding instruments. The International Maritime Organization (IMO), for example, has proposed over twenty treaties to deal with important issues of maritime safety or efficiency, most of which have been widely ratified. In addition, the AIIP Council would be authorized to create

and implement, with the Assembly's support, assistance programs to help needy States Parties participate effectively in the activities contemplated in the Stanford Draft.

The standards and recommendations to be developed by the AIIP would be designed to have the same legal force attributed to SARPs developed by ICAO. SARPs adopted by ICAO are not legally-binding; they become part of appendices to the ICAO Convention, and States Parties are expected to implement them. States Parties are required, however, to advise other States Parties of their failure to implement SARPs, and the latter would be free to act to protect themselves from the potential consequences of a State's failure to abide by the standard or practice at issue. This type of arrangement has proved universally acceptable in civil aviation and in other areas of transnational regulation, to ensure that standards and practices proposed are thoroughly vetted, widely supported, and accepted voluntarily on the basis of sovereign self interest and mutuality of obligation.

Authority is provided in Article 12 to the AIIP in the Stanford Draft to enable it to discipline States Parties, or States that are non-Parties but are participating in the information infrastructure. Where a State acts or allows persons to act in a manner that undermines the objectives of the Draft, the Council is authorized to recommend sanctions, and the Assembly is authorized to impose them on a two-thirds vote, up to and including expulsion from the AIIP, and a recommendation to States of exclusion from the information infrastructure. While the Draft avoids regulating State conduct, actions that undermine its purposes, such as allowing persons to use a State's territory to launch attacks affecting other States, would allow the AIIP to exclude such States from membership or to recommend punishing persons and/or non-Party States by excluding them from participation in the international information infrastructure.

5. Protection of Individual Rights. Transnational regulation of the Internet raises several important issues related to privacy and other individual rights.<sup>36</sup> The Stanford Draft ensures that, at a minimum, individual rights afforded by States Parties are not adversely affected. No State Party has any duty under the Stanford Draft to act in any manner that might infringe upon the privacy or other human rights of any individual or entity, as defined by the law of that State. In addition, the Stanford Draft authorizes

---

<sup>36</sup> See Ekaterina A. Drozdova, "Civil Liberties and Security in Cyberspace," Chapter 5, *International Cooperation to Combat Cyber Crime and Terrorism* (forthcoming, Hoover Press).

States Parties to refuse or cease cooperation in investigations or prosecutions they consider politically motivated or unfair. It would also create a subcommittee of experts as part of the AIIP, assigned the task of following and reporting upon the protection of privacy and human rights. Finally, the Draft provides that certain, fundamental protections must be extended to individuals detained for violations of any offense covered by its terms, including notice to the representative of the State of which an accused is a national, and the right to such representative's assistance.

Efforts to protect privacy and other human rights will involve complications for States Parties, for private entities, and for the AIIP as an organization. Notions of privacy and the scope of procedural and human rights vary considerably among the States whose participation is needed for a workable international regime. These differences have led the Internet Alliance to conclude that a legally-mandatory regime on Internet crime would likely "wreak havoc" on privacy protections.<sup>37</sup> In fact, no such result is necessary to have effective multilateral cooperation. By allowing States Parties to insist on the preservation of national norms as a minimum level of protection, the Stanford Draft would preclude its use to deprive any person of rights granted by any State Party, and the problems anticipated will be analogous to those created under the air transport and other antiterrorism conventions. Just as the United States and USSR were able to live with such differences in those contexts, and still benefit from the agreements (for example, by securing extradition and prosecutions of hijackers), the Stanford Draft has been designed to enable States with radically different political values to work together on achieving mutually beneficial aims without sacrificing those values. If, however, a serious and unresolvable situation emerged in which, for example, the regime of technical and operational cooperation developed under the Draft was abused by a State in some manner, the Assembly is empowered to impose sanctions in Articles 12, 13, and 21, including expulsion from the AIIP or a recommendation against the offending State's participation in the international information infrastructure.

6. National Security. The Stanford Draft makes clear, in a manner similar to other multilateral agreements, that it is inapplicable to State conduct and national security affairs. A multilateral agreement on cyber crime will have novel, complex, and

---

<sup>37</sup> See "An International Policy Framework for Internet Law Enforcement and Security: An Internet Alliance White Paper" (May 2000), available at <<http://www.Internetalliance.org/policy/leswp.html>>.

important objectives apart from the possible use of cyber systems by States as military or intelligence tools. Efforts to control State conduct related to national security will be unhelpful in advancing the development of a multilateral approach to the problem of cyber crime, and unnecessary as well.<sup>38</sup> ICAO protects civilian aircraft from attack, and the ITU protects radio transmissions from interference. But these treaties do not attempt directly to control States in the conduct of their national security affairs. To the extent use of cyber technology as a weapon is a concern, existing arms control agreements, and treaties incorporating the laws of war, are all potentially applicable, as are the UN Charter provisions concerning the use of force.<sup>39</sup> The Draft does provide sanctions against conduct that undermines its purposes. If further measures need to be considered to limit the use of cyber technologies in areas of national security, those should be taken up separately and not used to hold hostage the development of a multilateral regime to advance the process of dealing with criminal activities harmful to all States, their peoples, and their economies.

7. Dispute Resolution. The Stanford Draft relies initially on consensual resolution of disputes through negotiation and mediation. States Parties unable to resolve their disputes consensually are required to submit to arbitration in any agreed form. The Stanford Draft contemplates that the Council of the AIIP will, after its creation,<sup>40</sup> propose for the Assembly's consideration an arbitration mechanism through which disputes would be resolved by expert panels designated in advance to hear and decide such matters, perhaps in the relatively informal manner preferred by the industry for resolving disputes over website domain names.<sup>41</sup>

---

<sup>38</sup> See "Developments in the Field of Information and Telecommunications in the Context of International Security," UN General Assembly Doc. A/54/213 (Aug. 10, 1999), pp. 8-10 (wherein the Russian Federation comments on UN initiative and warns against the creation of an "information weapon").

<sup>39</sup> See Gregory D. Grove, Seymour E. Goodman, Stephen J. Lukasik, "Cyber-attacks, Counter-attacks and International Law," 42 *Survival*, n. 14, *supra*.

<sup>40</sup> The Stanford Draft makes no effort to deal with the technical measures necessary to create the AIIP, which would presumably be similar to the steps taken when, for example, ICAO was created toward the end of World War II.

<sup>41</sup> See, e.g., *Noodle Time, Inc. v. Max Marketing*, DeC AF-0100 (Mar. 9, 2000), reported in Int'l Law in Brief (Apr. 1-14, 2000), available at <<http://www.asil.org/ilibindx.htm>> (an example of the procedure set up by Internet users (with U.S. government support) to apply the rules governing website domain names, as established in the Uniform Domain Name Dispute Resolution Policy).

8. Amendments. The Stanford Draft contains a standard treaty provision enabling the States Parties to propose and approve amendments as necessary and appropriate.

**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;

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. "cyber terrorism" means intentional use or threat of use, without legally recognized authority, of violence, disruption or interference against cyber systems, when it is likely that such use would result in death or injury of a person or persons, substantial damage to physical property, civil disorder, or significant economic harm;
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 observe 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, conforming 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.I.A.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 cooperation as a mitigating factor in determining the person's punishment; and entering into arrangements concerning immunities or non-prosecution 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 non-governmental 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 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 and 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 which 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 non-permanent 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.

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 DEPOSITORY 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, non-commercial 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 DEPOSITORY STATE] on \_\_\_\_\_ [DATE].

### **Abbreviations**

AIIP	Agency for Information Infrastructure Protection
CCIPS	Computer Crime and Intellectual Property Section (U.S. Dept. of Justice)
CERT	Computer Emergency Response Team
CISAC	Center for International Security and Cooperation (Stanford University)
COE	Council of Europe
CRISP	Consortium for Research on Information Security and Policy (Stanford University)
DOD	Department of Defense (U.S.)
FBI	Federal Bureau of Investigation (U.S. Dept. of Justice)
G-8	Group of Eight
ICAO	International Civil Aviation Organization
IETF	Internet Engineering Task Force
IMO	International Maritime Organization
ITU	International Telecommunication Union
NGO	Non-Governmental Organizations
SARP	Standards and Recommended Practices
UN	United Nations
UNDP	United Nations Development Program
U.S.	United States