CYBER SECURITY INDUSTRY ALLIANCE

Ratifying the European Convention on Cybercrime

Ratifying the European Convention on Cybercrime

Private Industry Coalition Urges Swift Consideration and Ratification of International Treaty by the U.S. Senate

CONTENTS

WHAT THE CYBERCRIME CONVENTION DOES

1. **Defines and prohibits cybercrime**
2. **Provides national legal procedures, investigation tools and human rights safeguards**
3. **Establishes regime for international cooperation**

SUMMARY

This briefing is from a private coalition of technology companies and related industry organizations. Members are described at the end of the briefing. The coalition is united by the desire for ratification of the Council of Europe's Convention on Cybercrime by the United States of America. The Convention is a treaty that was signed by the United States on November 23, 2001. President George W. Bush conveyed it to the Senate for advice, consent and ratification on November 17, 2003. The treaty document number is 108-11.

The Convention on Cybercrime is the first and only international treaty aimed to protect society from a new type of criminal act called cybercrime. A cybercrime is an illegal action to destroy or hamper use of critical information technology infrastructure such as computer or telephone networks. Cybercrime also includes the use of those digital resources to commit traditional crimes such as theft of identity, property or proprietary information.

Cybercrime poses a huge threat to global society. One reason is the profound, fundamental change by technology in the way people live, work and communicate. Cybercrime is more far-reaching than traditional crime because is transcends geographical and national boundaries. In recent years, fast-moving computer viruses and worms have temporarily disrupted business operations and emergency services worldwide. Corresponding losses have cost Americans billions of dollars. For example, a recent survey by Gartner reported that 57 million Americans have received email related to Internet fraud attacks called "phishing," resulting in direct losses of about $1.2 billion. Attacks like these are on a geometric rise.

Cybercrime is also challenging existing legal concepts, particular since it transcends sovereign borders. Cyber-criminals are often in places other than where their crime hits victims. The Council of Europe engineered the Cybercrime Convention to resolve these legal issues and promote a common, cooperative approach to prosecuting people who commit cybercrime. The Coalition urges the Senate to rapidly consider and ratify the Convention, providing the U.S. with legal tools to combat and prevent cybercrime against Americans.

THE COUNCIL OF EUROPE AND ITS CONVENTION ON CYBERCRIME

CONVENTION ON CYBERCRIME

First international treaty for cooperation in the investigation and prosecution of computer crimes

What It Is

The Council of Europe Convention on Cybercrime is the first multilateral treaty addressing the need for cooperation in the investigation and prosecution of computer crimes.

How It Was Developed

The Council of Europe is a negotiating forum established in 1949 to uphold and strengthen human rights, promote democracy and the rule of law in Europe. Its 44 sovereign state members include all the European Union. For years the United States has participated in many Council-sponsored conventions related to criminal matters.

The idea for the Convention on Cybercrime grew from studies by the Council of Europe in 1989 and 1995. The Council established a committee to draft the Convention, which was finished in May 2001 and opened for signing and ratification on November 23, 2001.

The United States was invited as an "observer" to the two studies and helped develop the final Convention, which included several drafts made available for public comment. Active U.S. participants in the development process included representatives from the Departments of Justice, State and Commerce who closely worked with other U.S. government agencies and interested private parties. U.S. government representatives also met with members of the U.S. technology and communications industry plus public interest groups during 2000 and 2001 to gather and incorporate comments on draft provisions of the Convention. Based on this feedback, the U.S. sought and obtained important revisions to the Convention and its Explanatory Report.

What It Says

The Convention on Cybercrime includes 48 articles divided into four chapters, summarized here from the Council of Europe's Explanatory Report to the Convention.

Chapter I – Use of terms

Defines computer system, computer data, service provider, and traffic data

Chapter II – Measures to be taken at the national level

The Convention provides a framework of measures for implementation by sovereign states. Like other multilateral conventions, language is flexible to allow for adaptation by a variety of legal systems.

Substantive law issues in Chapter II cover criminalization of computer or computer-related crime, including offences such as illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography and offences related to copyright and neighboring rights.

Procedural law issues, including common conditions and safeguards apply to offences committed by means of a computer system or the evidence of which that is in electronic form. Chapter II covers procedural powers such as expedited preservation of stored data, expedited preservation and partial disclosure of traffic data, production order, search and seizure of computer data, real-time collection of traffic data, interception of content data and jurisdiction provisions.

Chapter III – International cooperation

Chapter III is most important to the United States because it includes provisions for traditional and computer crime-related mutual assistance and extradition rules. Traditional mutual assistance includes situations where no legal basis exists between parties such as by treaty or reciprocal legislation. When legal basis exists, existing arrangements apply to assistance under this Convention. Procedural powers defined in Chapter II apply in both situations, subject to extra conditions. Chapter III includes provision for a specific type of transborder access to stored computer data, with consent and where publicly available. It also provides for establishing a 24x7 network to ensure speedy assistance among the Parties.

Chapter IV – Final provisions

The final clauses mostly repeat standard provisions in Council of Europe treaties.

Status

To become effective, the Convention on Cybercrime required ratification by five countries, at least three of whom were in the Council of Europe. Those conditions were met and the Convention was entered into force on July 1, 2004. As of August 1, 2004, Council of Europe members who have ratified the Convention include Albania, Croatia, Estonia, Hungary, Lithuania and Romania. There are 28 other members of the Council of Europe and 4 non-member countries (including the U.S.) who have not ratified the Convention.

WHY RATIFICATION NOW IS IMPORTANT

CSIA believes it is important for the U.S. Senate to quickly consider and ratify the Convention on Cybercrime for these reasons:

REASONS FOR ACTION

1. **Shows leadership**
2. **Requires no new legislation**
3. **Removes or minimizes legal obstacles**
4. **Denies "safe havens" to cybercriminals**
5. **Safeguards civil liberties**

Shows Leadership

Cybercrime affects global society. Due to the massive impact and borderless nature of cybercrime, it is crucial for sovereign powers to cooperate on investigating and prosecuting cybercriminals. The United States should show leadership in these efforts by ratifying the Convention now.

Requires No New Legislation

There is no new legislation required by the United States after its ratification of the Convention on Cybercrime. The Convention allows reservations and declarations by signatories for exemption from particular provisions that contradict national law. The U.S. has proposed six reservations and four declarations to protect the Constitutional rights of American citizens while ratifying the Convention. Each is detailed in Secretary of State Colin L. Powell's submittal letter to President Bush (see Resources section). With those stipulations, the United States will not require implementing new legislation after ratification of the Convention. The Senate may choose to ratify the Convention after adding other reservations and/or declarations during the consideration process.

Removes or Minimizes Legal Obstacles

Ratification now will remove or minimize legal obstacles to international cooperation that currently impede U.S. investigations and prosecutions of computer-related crime.

Denies "Safe Havens" to Cybercriminals

The removal or minimization of legal obstacles through swift ratification will help deny "safe havens" to criminals and terrorists who can damage U.S. interests from abroad using computer systems.

Safeguards Civil Liberties

Ratification now will protect the privacy and civil liberties of Americans from efforts by foreign powers to investigate or prosecute incidents of alleged cybercrime based on political or religious motivations.

THE COALITION RECOMMENDS SPEEDY RATIFICATION OF THE CYBERCRIME CONVENTION

The Coalition urges Senate to take swift action on the following recommendations for the Council of Europe's Convention on Cybercrime:

RECOMMENDATIONS TO U.S. SENATE

- **Hold hearings**
- **Conclude consideration**
- **Ratify the Convention**

Hold hearings to complete the treaty consideration process. The Senate's Committee on Foreign Relations held an introductory meeting on the Cybercrime Convention on June 17, 2004. CSIA urges the Senate to continue consideration without delay.

Conclude consideration process of the Convention and proposed six reservations and four declarations. Accept and/or modify reservations or declarations as the Senate deems appropriate.

Ratify the Convention with a vote of the full Senate.

RESOURCES

Convention on Cybercrime

http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

Explanatory Report to the Convention on Cybercrime

http://conventions.coe.int/Treaty/en/Reports/Html/185.htm

Council of Europe

www.coe.int/DefaultEN.asp

President George W. Bush's treaty submittal letter to U.S. Senate and Secretary of State Colin L. Powell's submittal letter to President Bush

http://frwebgate.access.gpo.gov/cgi-bin/useftp.cgi?IPaddress=162.140.64.88&filename=td011.pdf&directory=/diskb/wais/data/108_cong_documents

Frequently asked questions and answers to Convention on Cybercrime by the U.S. Department of Justice

www.usdoj.gov/criminal/cybercrime/COEFAQs.htm

ABOUT THE COALITION

The private industry coalition for ratification of the Convention on Cybercrime consists of several technology companies and industry trade organizations.

Cyber Security Industry Alliance (www.csialliance.org) is an advocacy group to enhance cyber security through public policy initiatives, public sector partnerships, corporate outreach, academic programs, alignment behind emerging industry technology standards and public education. Launched in February 2004, the CSIA is the only public policy and advocacy group comprised exclusively of security software, hardware and service vendors that is addressing key cyber security issues. Members include BindView Corp.; Check Point Software Technologies Ltd.; Citadel Security Software Inc.; Citrix Systems, Inc.; Computer Associates International, Inc.; Entrust, Inc.; Internet Security Systems Inc.; iPass, Inc.; Juniper Networks, Inc., McAfee, Inc., PGP Corporation; Qualys, Inc.; RSA Security Inc.; Secure Computing Corporation Symantec Corporation and TechGuard Security.

Business Software Alliance (www.bsa.org) represents the world's leading developers of software, hardware and Internet technology, both in the United States and internationally. BSA's mission is to educate computer users on software copyrights and cybersecurity, advance public policy that fosters innovation and expands trade opportunities, and fight software piracy. BSA is headquartered in Washington, D.C. and is active in more than 65 countries. Members include Adobe Systems, Apple Computer, Autodesk, Avid, Bentley Systems, Borland International, Cisco Systems, CNC Software/Mastercam, Entrust, Hewlett-Packard, IBM, Intel, Internet Security Systems, Intuit, Macromedia, Microsoft, Network Associates, RSA Security, SolidWorks, Sybase, Symantec, UGS PLM Solutions and VERITAS Software.

Coalition's Organizing Sponsor:

Cyber Security Industry Alliance
2020 N. 14th Street
Suite 750
Arlington, VA 22201
703-894-1266
www.csialliance.org