109TH CONGRESS
1st Session

SENATE

EXEC. REPT.
109–6

COUNCIL OF EUROPE CONVENTION ON CYBERCRIME (TREATY DOC. 108–11).

NOVEMBER 8, 2005.—Ordered to be printed

Mr. LUGAR, from the Committee on Foreign Relations, submitted the following

REPORT

[To accompany Treaty Doc. 108–11]

The Committee on Foreign Relations, to which was referred the Council of Europe Convention on Cybercrime (Treaty Doc. 108–11) (hereafter "the Convention"), signed by the United States at Budapest on November 23, 2001, having considered the same, reports favorably thereon with six reservations and five declarations as indicated in the resolution of advice and consent, and recommends that the Senate give its advice and consent to ratification thereof, as set forth in this report and the accompanying resolution of advice and consent.

CONTENTS

I. PURPOSE

The Convention is the only multilateral treaty to specifically address computer-related crime and the gathering of electronic evidence. It is designed to enhance the investigation and prosecution of cross-border computer-related crimes by eliminating or reducing procedural and jurisdictional obstacles to international cooperation.

II. BACKGROUND

The growth of the Internet has brought with it a rising number of attacks on computer networks. The United States is heavily dependent on computer networks to support its critical infrastructure, including the military, satellite networks, transportation and communications systems, and large utilities. Attacks on these systems, as well as on U.S. Government networks, constitute a threat to U.S. economic and national security. Major U.S. financial institutions have also been the target of such attacks, resulting in significant financial losses. In addition to the threat to computer networks, computers increasingly have been used to conduct more traditional crimes, such as fraud, copyright piracy, and child pornography. Moreover, organized crime syndicates and terrorist groups have been known to use the Internet to facilitate planning and communications.

In 1997, the Council of Europe ("COE") responded to these problems by establishing the Committee of Experts on Crime in Cyberspace to negotiate a convention on cybercrime. This committee was composed of representatives of COE member states and four non-COE "observer" states (the United States, Canada, Japan, and South Africa). The United States expects the Convention to have significant law enforcement benefits and was a leading participant in the negotiations. The Council of Europe, at the urging of the United States and other countries, made several drafts publicly available and distributed comments it received to all negotiators for consideration. U.S. negotiators also received input directly from interested groups, including through several meetings they held with U.S. industry and other interested groups, such as privacy and civil liberties organizations.

The Committee of Experts finished its work in May 2001, and the Convention was adopted by the COE Committee of Ministers on November 8th of that year. On November 23, 2001, the Convention was opened for signature to all COE member states and the four observer states that participated in the negotiations, and was signed by 30 states, including the four observer states. The Convention entered into force on July 1, 2004, and now has 11 parties. Thirty-one other states have signed but not yet ratified the instrument. The Convention permits other non-COE member states to accede to the Convention, but only with the unanimous consent of all of its parties.

III. SUMMARY OF KEY PROVISIONS OF THE CONVENTION

A detailed article-by-article discussion of the Convention may be found in the Letter of Submittal from the Secretary of State to the President, which is reprinted in full in Treaty Document 108–11. A summary of the key provisions of the Convention is set forth below.

The Convention requires parties to prohibit certain computer-related crimes under their domestic laws, to develop certain investigative methods with respect to computer-related crimes and electronic evidence of other crimes, and to cooperate with other parties to investigate and prosecute such crimes.

Articles 2 through 6 of the Convention require parties to criminalize unauthorized access to a computer system; unauthorized interception of data from a computer system; unauthorized damage to or deletion of computer data; unauthorized interference with the operation of a computer system; and the possession, production, sale, procurement for use, import, distribution, or otherwise making available of devices designed to commit any of these offenses or of computer access information, such as passwords, with the intent that they be used to commit such offenses. In addition to these offenses related to computer security, articles 7 through 10 of the Convention obligate parties to establish the offenses of computer-related forgery and computer-related fraud, as well as various aspects of the production, possession, procurement, and distribution of child pornography using computers, and infringement of copyright and related rights by means of a computer and on a commercial scale. U.S. law already prohibits such conduct, and the reservations and declarations proposed by the committee (see Section VI below) would ensure that the United States may implement these obligations consistent with existing U.S. law.

Under articles 16 through 21 of the Convention, parties must develop and be prepared to use certain investigative techniques designed to improve the effective investigation of the crimes set forth under the Convention and other criminal offenses committed by means of computer systems, as well as the collection of electronic evidence of criminal offenses. These techniques include the ability to preserve, search, and seize stored computer data; the ability to collect in real time and preserve "traffic data" being communicated between computers; and the ability to intercept certain content of the data. It bears emphasis that all of these investigative tools are already provided for under U.S. domestic law. Therefore, the Convention will not establish new police powers in the United States or otherwise alter U.S. civil liberties protections. Article 15 of the Convention requires each party to ensure that the establishment, implementation and application of these powers and procedures are subject to conditions and safeguards to be provided for under its domestic law that adequately protect human rights and liberties. For the United States, the conditions and safeguards that would apply may be found in the U.S. Constitution, including particularly the Fourth and Fifth Amendments, and various federal statutes, such as those set forth in the Federal Rules of Criminal Procedure and Title 18 of the U.S. Code, which require, among other things, judicial supervision of any requests for interception or disclosure of electronic communications.

Article 15, paragraph 3 requires each Party, to the extent consistent with the public interest, to consider the impact of these powers and procedures on the rights, responsibilities and legitimate interests of third parties. In this regard, the committee notes that paragraph 148 of the explanatory report accompanying the Convention reflects the understanding of the Parties that such third parties include internet service providers. It states that "initial consideration is given to the sound administration of justice and other public interests (e.g. public safety and public health and other interests, including the interests of victims and the respect for private life). To the extent consistent with the public interest,

consideration would ordinarily also be given to such issues as minimising disruption of consumer services, protection from liability for disclosure or facilitating disclosure under this chapter, or protection of proprietary interests."

Chapter Three of the Convention addresses international cooperation, including extradition and mutual legal assistance among the parties. Article 24 of the Convention adds the crimes established under the Convention to those offenses for which extradition may be sought under extradition treaties in force among parties to the Convention, and permits, but does not require, parties to use the Convention as a basis for extradition in the absence of such treaties. For the United States, the Convention will not provide an independent legal basis for extradition, which will continue to be based on U.S. domestic law and applicable bilateral treaties. It will, however, effectively expand the scope of offenses covered under certain existing bilateral extradition treaties (those that specifically list the offenses for which extradition may be granted).

Articles 25 through 35 of the Convention relate to mutual legal assistance among the parties. Article 25 provides a general obligation that parties shall afford each other mutual assistance "to the widest extent possible for the purpose of investigations or proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form." Articles 29 through 31, and 33 provide specific obligations for such assistance, including assistance that would involve the use of the investigative techniques for collection of computerized evidence that articles 16 through 21 of the Convention oblige parties to establish under their domestic law. It should be noted that although article 34 permits parties to request assistance in the interception of content data, it is narrowly drawn; indeed, there is no general obligation to provide this form of cooperation, as assistance is available "only to the extent" already permitted by applicable mutual legal assistance treaties and domestic law. In the United States, that law is subject to close judicial supervision, and in no case will a foreign authority be able to obtain information on terms that are less restrictive than for U.S. law enforcement. Currently, there is no authority to intercept communications based solely on the request of a foreign government; the only instance in which the United States would be in a position to accommodate such a request would be if the interception of the communications were independently authorized as part of a related or parallel investigation in the United States, and disclosing the contents of the intercepted communications were otherwise appropriate (see 18 U.S.C. sec. 2517(7)). Under U.S. law, a search warrant is insufficient authority to intercept the content of communications in transmission, as that collection is governed by the wiretap and interception statutes (18 U.S.C. sec. 2510, et seq.), as noted above. Although a search warrant may be used to obtain stored data, it must involve a crime recognized under U.S. law.

Notably, assistance in collecting electronic evidence is not limited to the crimes established in the Convention, and the Convention does not require, as a precondition to assistance, that the offense being investigated also constitute a crime in the state receiving the request ("dual criminality"). This lack of a dual criminality require-

ment is hardly a novelty. In the last two decades, the Senate has approved, and the President has ratified, 43 bilateral mutual legal assistance treaties that do not contain such a requirement for all types of cooperation. This is in the interest of U.S. law enforcement, which aggressively utilizes these treaties to gain evidence abroad and would be hamstrung by a rigid dual criminality provision in all cases. Therefore, the United States will be able to use this Convention to obtain electronic evidence in cases involving money laundering, conspiracy, racketeering, and other offenses under U.S. law that may not have been criminalized in all other countries.

At the same time, the Convention contains sufficient safeguards to ensure that the lack of a "dual criminality" requirement will not result in the provision of assistance by the United States in any inappropriate situations. The Convention provides the same high standard of protection of U.S. Constitutional interests that is contained in U.S. bilateral MLATs. Assistance is to be provided in accordance with the provisions of mutual legal assistance treaties between the parties where they exist. Where no such treaties exist between parties, article 27 of the Convention provides a procedural mechanism for cooperation to be applied between them, including the grounds for refusal of such requests (in addition to any grounds provided under the law of the requested party). The grounds for refusal contained in paragraph 4 of article 27 are analogous to those contained in U.S. bilateral MLATs. A requested party may refuse any request concerning a political offense or that is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. In response to questions from the committee, executive branch officials confirmed that this provision authorizes the United States to deny a request where providing the assistance would impinge on U.S. Constitutional protections, such as free speech, and that the executive branch intends to deny assistance in such situations. In addition, they committed that "[T]he Department of Justice will carefully review each request, regardless of the country from which it comes, to ensure that compliance with it would not impinge on U.S. fundamental principles and policy, and that U.S. implementation of foreign requests would not be inconsistent with Constitutional protections."

The committee also wishes to emphasize that the United States will not rely upon authorities created in the USA PATRIOT Act to meet its obligations under the Convention. The Convention was substantially drafted prior to the enactment of the USA PATRIOT Act, and is entirely consistent with United States law as it existed at that time. Accordingly, for example, the Convention does not require, and the United States does not contemplate, the use of the delayed notice search warrants authorized by Title 18, United States Code, Section 3103a for implementation of the Convention. Similarly, because the Convention will be implemented consistent with existing procedures for mutual legal assistance, the United States does not and will not use tools authorized under Foreign Intelligence Surveillance Act procedures or administrative subpoenas to meet its treaty obligations. Instead, longstanding statutory and mutual legal assistance treaty and agreement procedures will be used consistently with the judicial oversight provided under those

treaties and laws, in full compliance with the rights guaranteed under the United States Constitution. For example, as with domestic cases, U.S. execution of foreign government requests for collection or disclosure of electronic evidence would require judicial oversight.

The Convention is expected to improve computer security without creating an undue burden on internet service providers ("ISPs"). The Convention does not impose any general requirement on ISPs to collect or retain data. Rather, in specific cases, they may be required to collect, preserve, or disclose specified data, just as they are under existing U.S. procedural law. In response to questions posed by the committee, executive branch officials indicated that the Department of Justice will continue its current practice under other mutual legal assistance instruments of reviewing requests for assistance and alerting the ISPs as to the appropriate urgency of such requests. They also confirmed that the Convention will have no effect on existing U.S. law or policy governing reimbursement of costs incurred by ISPs in responding to such requests.

The committee notes that articles 24, 25, 27 through 31, and 33 of the Convention, on extradition and mutual legal assistance, are intended to operate in the same way as similar provisions contained in bilateral extradition and mutual legal assistance treaties. As with such provisions in bilateral treaties, these provisions are self-executing. They will be implemented by the United States in conjunction with applicable federal statutes. Additionally, the executive branch has indicated that they are not intended to create any private rights of action. The committee notes that the lack of a private right of action does not affect the ability of a person whose extradition is sought to raise any available defense in the context of the extradition proceeding.

IV. Implementing Legislation

No new implementing legislation is required for the Convention. An existing body of federal laws will suffice to implement the obligations of the Convention, although some minor reservations and declarations are needed, as discussed below.

V. Committee Action

The Committee on Foreign Relations held a public hearing on the Convention on June 17, 2004, at which it heard testimony from representatives of the Departments of State and Justice (S. Hrg. 108–721). On July 26, 2005, the committee considered the Convention and ordered it favorably reported by voice vote, with the recommendation that the Senate give its advice and consent to its ratification, subject to the reservations and declarations contained in the resolution of advice and consent.

VI. Committee Recommendation and Comments

The Committee on Foreign Relations believes that the proposed Convention is in the interest of the United States and urges the Senate to act promptly to give advice and consent to its ratification, subject to the reservations and declarations contained in the resolution of advice and consent.

The committee has included a number of reservations and declarations in the resolution of advice and consent. Section two of the resolution contains six reservations. The first four reservations relate to the obligations under articles 4 (data interference), 6 (misuse of devices), 9 (offenses related to child pornography) and 10 (offenses related to infringements of copyright and related rights) of the Convention to criminalize certain conduct. Consistent with the recommendations of the executive branch, the committee has included these four technical reservations permitted by the Convention in order to ensure that the United States may implement these obligations consistent with existing U.S. law.

The fifth reservation concerns the scope of the Convention. Article 22 of the Convention requires each party to establish jurisdiction in respect of the offenses established under the Convention when committed in its territory or on board a vessel flying its flag or an aircraft registered under its laws. U.S. law does not expressly extend U.S. jurisdiction over these particular crimes when committed on board U.S. vessels and aircraft outside of U.S. territory, although in certain cases U.S. jurisdiction may exist on other jurisdictional bases. Because the United States cannot ensure its ability to exercise jurisdiction in all such cases, the committee concurs with an executive branch recommendation that the United States enter a reservation limiting the obligation of the United States consistent with the reach of U.S. law, as permitted by the Convention.

The sixth reservation relates to the federal system in the United States. Although U.S. federal law prohibits the conduct proscribed by the Convention, federal criminal law generally covers conduct involving interstate or foreign commerce or another important federal interest. Because U.S. state, not federal law, would apply to a narrow category of conduct that does not implicate a foreign, interstate, or other federal interest (e.g., an attack on a stand-alone computer), the executive branch recommended that the United States reserve against these obligations in these narrow circumstances, as permitted by the Convention. The committee agrees with this recommendation.

Section three of the resolution contains five declarations. The first three declarations relate to the obligations under articles 2 (illegal access), 6 (misuse of devices) and 7 (computer-related forgery) of the Convention to criminalize certain conduct. Consistent with the recommendations of the executive branch, the committee has included these three technical declarations permitted by the Convention in order to ensure that the United States may implement these obligations consistent with existing U.S. law.

The fourth declaration relates to procedures to be followed in the case of urgent requests for mutual legal assistance. Article 27, paragraph 9(a) of the Convention permits urgent requests to be made directly to the judicial authorities of a party unless, for efficiency reasons, that party declares at the time of ratification that such requests should instead be sent to its central authority. The committee concurs with the executive branch recommendation that the United States make such a declaration.

The last declaration relates to U.S. implementation of the Convention under existing U.S. law. The executive branch recommended that the United States include an understanding to

clarify that the United States intends to comply with the Convention based on existing law. The committee has included such a statement in the resolution, formulated as a declaration in accordance with recent committee practice.

Under article 37, any State not a member of the Council of Europe and which has not participated in the formulation of the Convention may accede to it, but it may only do so upon invitation. Such invitation requires the unanimous consent of the parties to the Convention. The United States would therefore have a voice in the accession of any state. While the committee believes that broad adherence to the Convention among both members and non-members of the Council of Europe could be beneficial to U.S. law enforcement interests, it has concerns about potential mutual legal assistance relationships with authoritarian states. The Convention provides a broad framework for sharing of electronic evidence—not merely that involving cyber-crime—and is thus a significant legal assistance tool. The committee believes that, given the nature of the evidence-sharing requirements in the Convention, it is important that the United States, in consultation with other parties, work to ensure that all parties "accept the principles of the rule of law," as the Council of Europe requires of its own members.

VII. Text of Resolution of Advice and Consent to Ratification

Resolved (two-thirds of the Senators present concurring therein),

SECTION 1. SENATE ADVICE AND CONSENT SUBJECT TO RESERVATIONS AND DECLARATIONS

The Senate advises and consents to the ratification of the Council of Europe Convention on Cybercrime ("the Convention"), signed by the United States on November 23, 2001 (T. Doc. 108–11), subject to the reservations of section 2, and the declarations of section 3.

SECTION 2. RESERVATIONS

The advice and consent of the Senate under section 1 is subject to the following reservations, which shall be included in the United States instrument of ratification:

(1) The United States of America, pursuant to Articles 4 and 42, reserves the right to require that the conduct result in serious harm, which shall be determined in accordance with applicable United States federal law.

(2) The United States of America, pursuant to Articles 6 and 42, reserves the right not to apply paragraphs (1)(a)(i) and (1)(b) of Article 6 ("Misuse of devices") with respect to devices designed or adapted primarily for the purpose of committing the offenses established in Article 4 ("Data interference") and Article 5 ("System interference").

(3) The United States of America, pursuant to Articles 9 and 42, reserves the right to apply paragraphs (2)(b) and (c) of Article 9 only to the extent consistent with the Constitution of the United States as interpreted by the United States and as provided for under its federal law, which includes, for example, crimes of distribution of material considered to be obscene under applicable United States standards.

(4) The United States of America, pursuant to Articles 10 and 42, reserves the right to impose other effective remedies in lieu of criminal liability under paragraphs 1 and 2 of Article 10 ("Offenses related to infringement of copyright and related rights") with respect to infringements of certain rental rights to the extent the criminalization of such infringements is not required pursuant to the obligations the United States has undertaken under the agreements referenced in paragraphs 1 and 2.

(5) The United States of America, pursuant to Articles 22 and 42, reserves the right not to apply in part paragraphs (1)(b), (c) and (d) of Article 22 ("Jurisdiction"). The United States does not provide for plenary jurisdiction over offenses that are committed outside its territory by its citizens or on board ships flying its flag or aircraft registered under its laws. However, United States law does provide for jurisdiction over a number of offenses to be established under the Convention that are committed abroad by United States nationals in circumstances implicating particular federal interests, as well as over a number of such offenses committed on board United States-flagged ships or aircraft registered under United States law. Accordingly, the United States will implement paragraphs (1)(b), (c) and (d) to the extent provided for under its federal law.

(6) The United States of America, pursuant to Articles 41 and 42, reserves the right to assume obligations under Chapter II of the Convention in a manner consistent with its fundamental principles of federalism.

SECTION 3. DECLARATIONS

(1) The advice and consent of the Senate under section 1 is subject to the following declarations, which shall be included in the United States instrument of ratification:

(a) The United States of America declares, pursuant to Articles 2 and 40, that under United States law, the offense set forth in Article 2 ("Illegal access") includes an additional requirement of intent to obtain computer data.

(b) The United States of America declares, pursuant to Articles 6 and 40, that under United States law, the offense set forth in paragraph (1)(b) of Article 6 ("Misuse of devices") includes a requirement that a minimum number of items be possessed. The minimum number shall be the same as that provided for by applicable United States federal law.

(c) The United States of America declares, pursuant to Articles 7 and 40, that under United States law, the offense set forth in Article 7 ("Computer-related forgery") includes a requirement of intent to defraud.

(d) The United States of America declares, pursuant to Articles 27 and 40, that requests made to the United States of America under paragraph 9(e) of Article 27 ("Procedures pertaining to mutual assistance requests in the absence of applicable international agreements") are to be addressed to its central authority for mutual assistance.

(2) The advice and consent of the Senate under section 1 is also subject to the following declaration:

The United States of America declares that, in view of its reservation pursuant to Article 41 of the Convention, current United States federal law fulfills the obligations of Chapter II of the Convention for the United States. Accordingly, the United States does not intend to enact new legislation to fulfill its obligations under Chapter II.

○