Order Code RS21208
April 26, 2002

Cybercrime: The Council of Europe Convention

Kristin Archick
Consultant, European Affairs
Foreign Affairs, Defense, and Trade Division

Summary

Thirty-three countries–including the United States–have signed the Council of Europe's Convention on Cybercrime of November 2001. The Convention seeks to better combat cybercrime by harmonizing national laws, improving investigative abilities, and boosting international cooperation. Supporters argue that the Convention will enhance deterrence, while critics counter it will have little effect without participation by countries in which cybercriminals operate freely. Others warn it will endanger privacy and civil liberties.

This report will be updated as events warrant. Future questions may be directed to Paul Gallis.

Background

The Council of Europe's Convention on Cybercrime was opened for signature on November 23, 2001.[1] The Convention is the first international treaty designed to address several categories of crimes committed via the Internet and other computer networks. Negotiations on the Convention began in 1997, following a determination by the Council that the transnational character of cybercrime could only be tackled at the global level. Since then, the increase in hacking incidents, the spread of destructive computer viruses, and the minimal prosecution of such crimes in many states, have spurred on the Council's efforts. The September 11 terrorist attacks provided further momentum by raising the specter of cyber attacks on critical infrastructure facilities, financial institutions, or government systems, and by highlighting the way terrorists use computers and the Internet to communicate, raise money, recruit, and spread propaganda. To date, the Convention

[1] The Council of Europe has 43 member states–including all 15 members of the European Union–and seeks to promote and protect human rights and the rule of law throughout Europe.

has been signed by 29 Council of Europe members and four non-members (the United States, Canada, Japan, and South Africa) that also participated in the negotiations.[2]

The Convention's main goal is to establish a "common criminal policy" to better combat computer-related crimes worldwide through harmonizing national legislation, enhancing law enforcement and judicial capabilities, and improving international cooperation. To these ends, the Convention requires signatories to:

- *Define criminal offenses and sanctions under their domestic laws for four categories of computer-related crimes*–fraud and forgery, child pornography, copyright infringements, and security breaches such as hacking, illegal data interception, and system interferences that compromise network integrity and availability. Signatories must also enact laws establishing jurisdiction over such offenses committed on their territories, registered ships or aircraft, or by their nationals abroad.

- *Establish domestic procedures for detecting, investigating, and prosecuting computer crimes, and collecting electronic evidence of any criminal offense.* Such procedures include the expedited preservation of computer-stored data and electronic communications ("traffic" data), system search and seizure, and real-time interception of data. Parties to the Convention must guarantee the conditions and safeguards necessary to protect human rights and the principle of proportionality.

- *Establish a rapid and effective system for international cooperation.* The Convention deems cybercrimes to be extraditable offenses, and permits law enforcement authorities in one country to collect computer-based evidence for those in another. It also calls for establishing a 24-hour, seven-days-a-week contact network to provide immediate assistance with cross-border investigations.

Next Steps

The Convention will enter into force once it has been ratified by five states, including at least three Council of Europe members. It has not yet been ratified by any signatory. Following its entrance into force, the Council–in consultation with the four non-member signatories–may then invite other states to accede to the Convention.

The Council is currently drafting an additional protocol to the Convention that would define racist or xenophobic acts committed through computer networks as criminal offenses and prohibit distributing racist material via the Internet. The draft Convention contained language–supported by several European countries–criminalizing racist web sites, but this provision was dropped when the United States resisted its inclusion on freedom of speech grounds. As a result, negotiators agreed to address computer-related

---

[2] The 29 Council of Europe member state signatories are: Albania, Armenia, Austria, Belgium, Bulgaria, Croatia, Cyprus, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Macedonia, Malta, Moldova, the Netherlands, Norway, Poland, Portugal, Romania, Spain, Sweden, Switzerland, Ukraine, and the United Kingdom.

hate speech in a protocol, which the United States and others could choose not to sign. Last November, the Council of Europe's parliamentary assembly also recommended strengthening the Convention to permit the interception and decoding of electronic messages between suspected terrorists. The Council has not yet reached a decision on whether to pursue this course of action.

Possible Benefits and Risks

Convention supporters argue that it represents a significant step forward in tackling cybercrime because it commits signatories to prosecute computer-related crimes vigorously–which many countries fail to do currently. Council of Europe officials say that the Convention will end cybercriminals' "feeling of impunity."[3] They claim that by mandating sanctions and making cybercrimes extraditable offenses, the Convention will improve deterrence and reduce the number of countries in which criminals can avoid prosecution. Advocates also argue that the Convention's procedures for collecting evidence will assist law enforcement authorities in the fight against terrorism.

Skeptics, however, point out that in order to serve as a deterrent, more states will have to sign the Convention and abide by its mandates. They note that the states that participated in the Convention's negotiations are not the "problem countries" in which cyber criminals operate relatively freely. Hackers frequently route cyber attacks through portals in Yemen or North Korea, neither of which are part of the Convention. The Filipino author of the "I Love You" virus that caused millions of dollars in damage worldwide in 2000 was never prosecuted because no applicable laws existed. In addition, some analysts criticize the Convention for not permitting police authorities direct cross-border access to computer data, which they argue creates an extra, time-wasting step.[4]

The Convention has also come under fire from civil liberties groups concerned that it undermines individual privacy rights and expands surveillance powers too far. The American Civil Liberties Union claims that U.S. authorities will use the Convention to conduct surveillance and searches that would not be permitted under current U.S. law. European critics worry that the Convention allows the transfer of personal data to countries outside Europe–such as the United States–that they believe have less protective laws regarding the use of such information. Council of Europe officials dismiss such fears, arguing that the Convention provides adequate civil liberty safeguards and limits information transfers to specific criminal investigations. Meanwhile, some business and consumer groups are concerned that the Convention's provisions could increase costs to service providers, impede the development of security technologies and sale of encryption programs, and negatively affect consumer confidence in e-commerce.

---

[3] "European cybercrime pact aims to set global benchmark," AFP, November 22, 2001.

[4] William New, "Privacy agenda in 2002 has international flavor," *National Journal Technology Daily*, January 23, 2002; "Under antiterror law, government can use U.S. standards to nab foreign hackers," AP, November 21, 2001.

U.S. Policy

Both the Clinton and Bush Administrations worked closely with the Council of Europe on the Convention. U.S. officials believe that it "removes or minimizes the many procedural and jurisdictional obstacles that can delay or endanger international investigations and prosecutions of computer-related crimes."[5] The Bush Administration was pleased with the Convention's data preservation approach, which requires the storage of specified data–relevant to a particular criminal investigation and already in a service provider's possession–for a limited period of time. It views this provision–currently lacking in many national laws–as key to improving the counter-terrorist capabilities of law enforcement officials worldwide.[6]

The Bush Administration has not yet submitted the Convention to the Senate for ratification. U.S. legal analysts believe that the Convention will not require much, if any, implementing legislation because American negotiators succeeded in scrapping most objectionable provisions–such as the hate speech article–thereby ensuring that the Convention tracks closely with existing U.S. laws.

Proponents assert that many of the Convention's provisions reflect the spirit of several bills passed or pending in the Congress that relate to cybercrime, cyberterrorism and cybersecurity:

- The USA PATRIOT ACT (**P.L. 107-56**, introduced as **H.R. 3162** by Rep. James Sensenbrenner in October 2001) authorizes the interception of electronic communications for the collection of evidence related to terrorism, computer fraud, and abuse (Sections 201 and 202). It also clarifies the definition of protected computers and increases fines and prison terms for damage (Section 814).

- **H.R. 3482** (Cyber Security Enhancement Act of 2001; introduced by Rep. Lamar Smith in December 2001) calls for increased penalties–up to life in prison–for cybercrimes that result in death or serious bodily injury as well as stiffer sentences for other hacking offenses.

- **S. 1900** (Cyberterrorism Preparedness Act of 2002; introduced by Senator John Edwards in January 2002) directs the National Institute of Standards and Technology to award a five-year grant to a nongovernmental entity to carry out a national program aimed at protecting the U.S. information infrastructure and to develop cybersecurity best practices.

---

[5] U.S. Department of Justice, "Frequently Asked Questions and Answers About the Council of Europe Convention on Cybercrime" [http://www.usdoj.gov/criminal/cybercrime/newcoefaqs.html].

[6] The United States draws a distinction between *data preservation* and *data retention*. The latter requires service providers to routinely collect and keep all or a large portion of traffic. The United States largely opposes broad data retention regimes, but views preservation as striking a good balance between the needs of law enforcement, business interests, and privacy rights.