

The Council of Europe Cybercrime Convention
Entered into force January 2004

James A. Lewis

Center for Strategic and International Studies

Two and a half years after the Council of Europe Cybercrime convention entered into force, the United States has ratified it.

Faced with the explosive growth and commercialization of the Internet in the 1990s, law enforcement agencies in many countries concluded that their domestic laws were inadequate for a new kind of crime – cybercrime.¹ Someone sitting before a computer in one country could access computer networks in another country to commit crimes in a third - a “transnational” or “transborder” crime. One review of fifty countries found that two thirds had inadequate cybercrime laws. Procedures for bilateral law enforcement cooperation did not always cover computer crimes and were often too slow to be of use. Cybercrime is part of a larger transnational challenge to law enforcement and the authority of national governments created by the revolution in information technology, easy international travel, and the growth of extensive financial and trade networks. These challenges can be met only when nations cooperate.

The diplomatic tools developed for the last century for police in one country to request the assistance of police and courts in another– Letters Rogatory or Mutual Legal Assistance Treaties - are slow and do not help when national laws are incompatible. Many countries still lack an adequate legal framework for the deterrence and punishment of cybercrimes or rely on an uneven patchwork of legislation. Disagreement over what constitutes a crime; inadequate, uneven or absent authorities for governments to investigate and prosecute cybercrime; and procedures for international cooperation more attuned to the age of sail than to the Internet have hampered international cooperation on cybercrime.

The transnational aspect of crime is compounded by technological developments that pose new and difficult challenges for law enforcement. Digital evidence is fragile and transitory and old techniques for wiretapping no longer work. Police agencies in the U.S. and elsewhere have felt beleaguered as global forces and new technologies erode their ability to enforce the law.

The U.S. Department of Justice began in the 1990s to work with the Organization for Economic Cooperation and Development and the G-8 to develop cooperative responses to cybercrime. The Council of Europe, which has a mandate to promote the rule of law and human rights, began a similar effort in the late 1980s. In 1995, the Council’s European Committee on Crime Problems recommended adoption of an international treaty on cybercrime. In February 1997, the Council of Europe created a new committee (the Committee

¹ The Convention defines cybercrime as offences committed against “the integrity, availability, and confidentiality of computer systems and telecommunication networks” (e.g. the Internet), or the use of networks or their services to commit traditional offences, including money laundering, offering illegal services, violation of copyright, violations of “human dignity (e.g. racism) and the protection of minors.”

of Experts on Crime in Cyberspace) to prepare a binding convention that addressed offences, criminal law, and jurisdiction. The United States was invited to be an active participant in the cybercrime effort along with Japan, Canada and South Africa.

At first, this effort attracted little public notice. To its credit, the Council made the drafting process unusually open (by diplomatic or business standards). The Committee released a draft convention to the public (including publication on the Internet - one advantage of the Internet is that it allows texts to be circulated widely for comment – a kind of ‘open-source’ diplomacy) and held a public hearing in March 2001.

The draft tapped a deep reservoir of concern over government intrusiveness and prompted an energetic public response. Corporations and cyber-libertarians found themselves allies in opposing the Convention. Twenty-two privacy and business associations in Europe, the United States, Japan, Australia and South Africa created the “Global Internet Liberty Campaign” to oppose the Convention. UNESCO (concerned over the extension of criminal penalties to copyright infringement) and the European Union’s Privacy Working Group also offered objections to the draft convention’s piracy and data preservation provisions.

The critics’ view was that the Convention was fundamentally imbalanced, as it provided sweeping powers for computer search and seizure and communications surveillance without corresponding protections for privacy and civil liberties. Information Technology groups feared that implementing the Convention would be costly, but Entertainment industry groups said that the Convention’s copyright provisions would help the battle against cross-border Internet crime. Civil liberties groups stated that the Convention could lead to a curtailment of freedom of expression online and gave too many investigative powers to police and government organizations.

Business concerns were driven by the potential expense of data-preservation requirements (such as requiring service providers to preserve e-mail routing data). The Convention’s data preservation provisions could increase costs and force Internet Service Providers and other firms to reshape their businesses in ways that were favorable to law enforcement, to guarantee surveillance and data recovery. The difficult U.S. experience with the “Clipper Chip” and the Communications Assistance to Law Enforcement Act (which requires U.S. telephone companies to build wiretap capacity in their networks) helped prompt this. The lack of adequate privacy protections for Americans may have also contributed to fears of misuse of data collected by law enforcement. IT companies were also concerned that the Convention would result in their being liable for criminal actions that used their networks.

Early drafts of the Convention also had very broad definitions of criminal conduct that covered a wide range of legitimate behaviors. One section made it an offense to access any computer without permission, effectively if inadvertently criminalized web surfing. In a similar vein, the draft's provisions on "Illegal Devices" were drafted so as to apply to security tools as well as hacking tools.

The extraterritorial application of national laws also raised concerns. Cyberspace may not have any borders, but the computer networks that comprise it are physically located in countries and

subject to their laws. A signatory to the Convention could request assistance in investigating an act that was a crime under its laws but not in the jurisdiction of the nation it was asking for assistance (i.e. an absence of “dual-criminality”). Critics said that a dual criminality provision was “central to preserving the sovereign authority of nations.” They called for limitations, clear procedures and a high level of individual rights protections for international investigations taken under the Convention.

The most prominent issue was the implication for privacy of the provision on police surveillance powers and digital evidence preservation. The ability of governments to intrude on the privacy of their citizens has been greatly enhanced by new technologies. The Cybercrime convention was sometimes portrayed as creating Orwellian police powers, and commercial interests echoed these concerns to buttress their opposition to assuming new costs and responsibilities.

There are major differences between U.S. and European attitudes on the role of the State and on privacy. In the United States the most vocal concerns are over police ‘wiretapping’ of communications, including the Internet. In Europe, there is greater concern over personal data being exploited for commercial use (many European countries allow their internal security agencies much greater freedom in wiretapping than does the U.S.). Communications interception has been an essential weapon against crime and terrorism for decades and the Convention only accelerated and formalized efforts by most countries to extend telephone wiretap capabilities to Internet based communications.

Another major difference lay in the dissimilarities of Napoleonic law and the United States approach to common law, with its emphasis on due process and individual rights. Where Europeans sometimes saw U.S. law as inadequate in protecting privacy, European laws did not provide the same level of formal protection for civil liberties found in the United States. Bringing Napoleonic and Common-law systems into alignment was a fundamental challenge in drafting the Convention. If the United States had not participated, the final convention would have looked very different, with a much more Napoleonic (and perhaps draconian) cast.

The final draft was modified substantially to address these concerns (albeit not to the satisfaction of many critics). The Convention supplements multilateral and bilateral agreements, harmonizes national laws for cybercrime, sets the basis for common powers of investigation and “fast and effective” international co-operation. It defines four categories of cybercrime to be covered by signatories’ national laws:

- 1) Crimes against the confidentiality, integrity and availability of computer data and systems, including illegal access or interception, interference with data or systems, or misuse of devices;
- 2) Computer fraud or forgery;
- 3) Content-related crimes. This currently applies to child pornography, but the next step is a Protocol covering racist or xenophobic ideas on the Internet, an area of potential conflict for the U.S with its free-speech guarantees;

4) Intellectual property and copyright infringement crimes, such as the distribution of pirated copies.

One significant change in the final draft is an increased emphasis on rules and safeguards for mutual assistance.² Article 15 now binds signatories, when carrying out these functions, to observe their commitments to the Convention for the Protection of Human Rights and Fundamental Freedoms, the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, and the UN Covenant on Civil and Political Rights.

Language on “intent” was added to ensure that to qualify as criminal, an act must be committed deliberately and “without right.” Signatories have also agreed to establish a contact network among Justice Ministries to provide immediate investigatory assistance. The Convention does not, however, allow police in one country to conduct investigations in another (called “transfrontier investigations). Signatories must cooperate with requests for assistance in collecting computer evidence, but other provisions make clear that countries can refuse to disclose data if they believe this will prejudice their sovereignty, security or other essential interests, or where they consider the request to be related to a political act. Finally, countries can reserve on sections that are incompatible with their national laws when they sign the Convention, and all of its provisions will be reviewed three years after entry into force.

The Convention did not include “hate speech” among its cybercrimes, despite a strong desire to do so on the part of many Europeans. The main obstacle was First Amendment protections given to U.S. websites. One expert called for European governments to prevent the United States from become a “cyberhaven” for racism. Members of the Council suggested that the United States deny First Amendment protection to sites where content is provided in languages not destined for the American public, where content providers are not domiciled in the same country as the ISP and where visitors are principally based outside of the United States. The Europeans realize that this suggestion is incompatible with the First Amendment and that agreement with the Americans is unlikely, but they are moving at a rapid pace to add a protocol to the Convention this year to criminalize “acts of racist and xenophobic nature through computer networks” (e.g. production and dissemination of information on the Internet).

This protocol posed serious problems for the United States, not only because of the potential for conflict with the First Amendment, but also in the risk of setting a global precedent for prosecuting U.S. companies when they host content that another country finds offensive. Many European countries already have this authority (demonstrated by France’s prosecution of ‘Yahoo!’ for hosting Nazi websites and by similar cases in Italy and Germany), but the protocol could establish an international legal standard. The United States has little support and less leverage for its stance.

The dispute over this protocol should not detract from the benefits of the Convention. While it attracted much criticism during its long negotiation, it is the most concrete multilateral

² For the preservation of stored data; preservation and disclosure of traffic data; production orders; search and seizure of computer data; real-time collection of traffic data and interception of content.

achievement to date for building better cybersecurity. It is understandable that better cooperation among police forces can raise fears about privacy and human rights, but the Convention lets very different national legal systems cooperate in investigating and prosecuting cybercrime without yielding national sovereignty. It does this by creating both common definitions of cybercrime and formal processes for cooperation, while allowing nations the choice of opting out of specific investigations or provisions.

The Convention on Cybercrime was opened for signature on November 23, 2001. It entered into force in January 2004. Thirty nine countries have signed it and sixteen, including the U.S., have ratified it (five signatures were required for entry into force). Its rules will apply to most of the world's Internet traffic if it is ratified by the U.S, Canada, Japan and South Africa. Implementing the Convention will not be a challenge for the United States, as most of the authorities needed to conform to it are already found in U.S. law. Preventing unauthorized access to computer systems lies at the core of cybersecurity and critical infrastructure protection. Effective prosecution of cybercrime can reduce and deter unauthorized access. Cybercrime laws are only part of the solution – cybersecurity also requires better technology, clearer rules about identity and mechanisms for coordinated activities and information sharing.

Better security requires many countries to act in a coordinated fashion. Sovereignty – the decision of a group of people to govern themselves without external interference – remains a serious obstacle to cooperation. The Council of Europe Cybercrime Convention is a serious test of the ability to cooperate in Internet security and critical infrastructure protection. The Convention revealed substantial differences in national legal systems regarding fundamental issues for cyberspace. While these were successfully bridged in the Council negotiations, the Cybercrime Convention may show for now the limits of the possible in cyber-security cooperation.
