;login:
THE MAGAZINE OF USENIX & SAGE
February 2002 • Volume 27 • Number 1

inside:

THE WORKPLACE

The Law Moves In

by Edgar Danielyan

USENIX & SAGE
The Advanced Computing Systems Association &
The System Administrators Guild

the law moves in

by Edgar Danielyan

Edgar Danielyan is a Cisco-certified network, security, and design professional, as well as a certified paralegal. He is the author of *Solaris 8 Security* as well as many articles on the Internet, UNIX, and security.He is currently a self-employed consultant and author.

edd@danielyan.com

The Convention on Cybercrime

The Internet has long been perceived either as lawless cyberspace inhabited by hackers and criminals or as a modern-day utopia, ideal environment for freedom, democracy, and libertarianism. As always, the truth lies somewhere between these polar viewpoints. While empowering individuals to share and disseminate information and ideas freely, it is also a powerful tool and medium for all kinds of crimes – ranging from simple theft to terrorism and espionage. Fortunately, it seems something is finally being done by the governments to combat international cybercrime. This article briefly introduces the flagship move on this front: the Convention on Cybercrime, drafted by the Council of Europe and now signed by thirty states, both members and non-members of the Council. While it is too early to say whether this legal instrument will actually improve the current state of affairs, it is nonetheless the first of its kind and deserves consideration.

The Convention on Cybercrime

On paper, the Convention on Cybercrime seems to be what was needed to combat international cybercrime. It defines as criminal offenses certain acts, such as illegal access to systems and data, and provides the legal and procedural framework for the investigation and prosecution of persons committing these crimes. However, it will be up to national legislatures and courts to enact and enforce the provisions of the Convention, and economic, legal, and administrative differences between signatory states will inevitably mean that international prosecution of cybercriminals remains a tough task. There is no doubt that the Convention will be ratified sooner or later, and that the legal landscape will change considerably after it comes into effect. Hopefully, it will also convince those of us who don't believe in legal action against cybercriminals to at least try to prosecute them. In the meantime, corporate legal counsel and law firms should inform themselves about the possibilities and procedures introduced by the Convention and stay tuned for the day it becomes law.

The Convention on Cybercrime was adopted by the Committee of Ministers of the Council of Europe on 8 November 2001 after years of consultations and work on the document. Shortly thereafter, on 23 November 2001, the Convention was signed at the Hungarian Parliament in Budapest by the following thirty states: Albania, Armenia, Austria, Belgium, Bulgaria, Croatia, Cyprus, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Moldova, the Netherlands, Norway, Poland, Portugal, Romania, Spain, Sweden, Switzerland, Macedonia, Ukraine, United Kingdom, Canada, Japan, South Africa, and the United States. All these states, with the exception of Canada, Japan, South Africa and the United States, are members of the Council of Europe. The Convention itself, with its four chapters and forty-eight articles, is written in plain English and avoids legal language as much as possible. It will come into effect and become binding on the signatory states after ratification by national parliaments. As soon as five signatory states, at least three of which must be Council of Europe members, ratify the Convention, it will start its life as a working international legal instrument. In the preamble to the Convention, reference is made to the following international legal instruments which were taken into account by its drafters:

- European Convention for the Protection of Human Rights and Fundamental Freedoms (Council of Europe, 1950)
- International Covenant on Civil and Political Rights (United Nations, 1966)
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe, 1981)
- Convention on the Rights of Child (United Nations, 1989)
- Worst Forms of Child Labour Convention (International Labour Organization, 1999)

The influence of the European Convention on Human Rights (ECHR) on the Convention on Cybercrime is especially profound and may be seen in Article 15, "Conditions and safeguards." This article stipulates that all provisions of the Convention are subject to the protection of human rights and fundamental freedoms guaranteed by the ECHR. However, since these guarantees are only applicable in the member states of the Council of Europe, Article 15 expressly states that application of the powers and procedures provided for in the Convention is subject to the principle of proportionality. The Convention also provides for judicial or other independent supervision, and limitation on the scope and duration of powers and procedures arising from the Convention.

The influence of the European Convention on Human Rights (ECHR) on the Convention on Cybercrime is especially profound.

Chapter I: Use of Terms

Appreciating the fact that computer terminology may be a potential source of confusion, many concepts are first defined before being used. Article 1 of the Convention, entitled "Definitions," defines terms such as "computer system" and "computer data":

> "computer system": any device or a group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; "computer data": any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.

Chapter II: Measures to Be Taken at the National Level

SECTION 1: SUBSTANTIVE CRIMINAL LAW

Title 1: Offenses against the confidentiality, integrity and availability of computer data and systems

Articles 2-6 establish the following actions as criminal offenses: illegal access, illegal interception, illegal data interference, illegal system interference, and misuse of devices.

The term "illegal" is defined as action without right; in some cases, signatory states may require that such actions be committed with dishonest intent.

Title 2: Computer-related offenses

Articles 7-8 establish the following actions as criminal offenses: computer-related forgery, computer-related fraud.

"Fraud" is defined in Article 8 as "any input, alteration, deletion, or suppression of computer data; any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another."

Title 3: Content-related offenses

Article 9 defines as criminal any offenses related to child pornography. For the purposes of this article, "children" includes all persons under 18 years of age. By a reservation to the Convention, however, a party may require a lower age limit, which shall be not less than 16 years.

Title 4: Offenses related to infringements of copyright and related rights

Article 10 criminalizes infringement of copyright as defined by national law of member states pursuant to international obligations of member states.

Title 5: Ancillary liability and sanctions

Articles 11-13 establish as criminal offenses any attempt to commit, or to aid or abet the commission of, any of the offenses established by Articles 2-10; provide for corporate liability of legal persons; and provide for sanctions and measures intended to ensure that criminal offenses established by the Convention are punishable by effective, proportionate and dissuasive sanctions, which may include deprivation of liberty.

Section 2: Procedural law

Title 1: Common provisions

Articles 14-15 specify the general principles of procedural law and define the scope of applicability; specify the conditions and safeguards for the application of the Convention with reference to the norms enshrined in the European Convention on Human Rights.

Title 2: Expedited preservation of stored computer data

Articles 16-17 deal with expedited preservation of stored computer data and disclosure of traffic data.

Title 3: Production order

Article 18 covers interjurisdictional production orders.

Title 4: Search and seizure of stored computer data

Article 19 defines how computer data can be searched and seized.

Title 5: Real-time collection of computer data

Articles 20-21 cover real-time collection of traffic data and data interception.

Section 3: Jurisdiction

Article 22 deals with questions of jurisdiction of states in accordance with Articles 2-11 of the Convention.

Chapter III: International Cooperation

Section 1: General principles

Title 1: General principles relating to international cooperation

Article 23 stipulates that signatory states shall cooperate with each other to the extent provided for in their international agreements.

Title 2: Principles relating to extradition

Article 24 defines the procedures and requirements for extradition for criminal offenses established by Articles 2-11 of the Convention.

Title 3: General principles relating to mutual assistance

Articles 25-26 specify when and how signatory states should or may offer mutual assistance in matters covered by the Convention.

Title 4: Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Articles 27-28 define how parties may offer mutual assistance when there are no mutual legal assistance treaties between them. In particular it provides for requests for assistance to be made through the International Criminal Police Organization (INTERPOL).

Section 2: Specific provisions

Title 1: Mutual assistance regarding provisional measures

Articles 29-30 deal with expedited preservation of stored computer data and disclosure of preserved traffic data.

Title 2: Mutual assistance regarding investigative powers

Articles 31-34 provide for mutual assistance in international investigations under this Convention.

Title 3: 24/7 Network

Article 35 provides for the establishment of 24/7 points of contact in all signatory states which are to provide assistance defined in the Convention. It also requires all parties to ensure that trained and equipped personnel are available to satisfy the requirements of this article.

Chapter IV: Final Provisions

Articles 36-48 deal with legal and administrative procedures of the Convention.

Summary

On paper, the Convention on Cybercrime seems to be what was needed to combat international cybercrime. It defines as criminal offenses certain acts, such as illegal access to systems and data, and provides the legal and procedural framework for the investigation and prosecution of persons committing these crimes. However, it will be up to national legislatures and courts to enact and enforce the provisions of the Convention, and economic, legal, and administrative differences between signatory states will inevitably mean that international prosecution of cybercriminals remains a tough task.

The full text of the Convention on Cybercrime may be obtained from the Council of Europe at *http://conventions.coe.int* along with its Explanatory Memorandum.