Chapter LIV
International Cybercrime Convention

Sylvia Mercado Kierkegaard
International Association of IT Lawyers (IAITL), Denmark

ABSTRACT

The Internet's global character and the increasing pressure from industries have prompted legislators to sort-out cross border cybercrime issues with a legislative solution—the CoE Convention on Cybercrime. The Convention on Cybercrime is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation. The convention is cause for concern as it gives governments too much power without any system of check and balance, and without protecting the civil liberties of web users.

INTRODUCTION

Information technology, in particular the Internet, provides great benefits for society. However, organized crime has become well established in cyberspace, using the Internet for human trafficking and other crimes. Governments and private sector officials from around the world are seeking ways to jointly combat cybercrime. Cyber criminals engage in activities such as selling access to networks of hacked personal computers (PCs) to send spam or launch attacks, or selling details of new security vulnerabilities so systems can be compromised. Security experts are increasingly concerned about the growing sophistication of the technology and techniques used by organized gangs of computer hackers and other criminals. The growth of cybercrime underscores the vulnerability of Internet users at a time when more and more people rely on the Web.

National boundaries are still too much of an obstacle to law enforcement. The paradox of the Internet—a worldwide computer network designed by visionaries and scientists—succumbing to hacking, phising and other forms of multijurisdictional cybercrime com-

mitted by teenagers and organized criminal elements riles law enforcement agents and government leaders. There is little doubt that computer crime and computer misuse is a growing malaise and has contributed to loss of business, competitive advantage, and privacy. The Internet's global character and the increasing pressure from industries have prompted legislators to sort out cross border cybercrime issues with a legislative solution—the Council of Europe (CoE) Convention on Cybercrime. This chapter will discuss the convention, its salient provisions, and possible impact on the cyber community. The aim of this chapter is to determine whether the treaty is an effective and rapid response to the growing threat of cybercrime, and whether these threats prompted by the borderless Web eventually could be resolved by a treaty.

CYBERCRIME

While "the emergence of new forms of computer crime has been widely noted in the press" (Michalowski, 1996), there is still no accepted definition of what really constitutes cybercrime. The 2005 *Oxford Dictionary of Law* defines cybercrime as "crime committed over the Internet. No specific laws exist to cover the Internet, but such crimes might include hacking, defamation over the Internet, copyright infringement, and fraud." *Encyclopaedia Britannica* defines it as "any use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy."

The definition of cybercrime is still evolving and has now been expanded to cover any illegal act involving a computer and to all the activities done with criminal intent in cyberspace or are computer related. There is a sharp disagreement among legal experts on whether cybercrime should only include new forms of crimes that have no offline equivalent.

Jurisprudence and Internet legislations are just emerging for managing computer-related crimes. Cybercrime is neither fully nor partially covered by most existing laws. For example, Reonel Ramones, authored the Love Bug virus, but was not prosecuted because the Philippines did not have then a law to deal with computer crime. The absence of uniform law is an issue that has crime fighters up in arms and has led the CoE and the United States to confront the legal problems at a multinational level through the harmonization of substantive criminal law and a coordinated approach.

Is Cybercrime Really a Menace?

Results from the 2005 E-Crime Watch survey reveals the fight against electronic crimes (e-crimes) may be paying off. The 2005 E-Crime Watch survey was conducted by *CSO* magazine in cooperation with the U.S. Secret Service and Carnegie Mellon University. The research was conducted to unearth e-crime fighting trends and techniques, including best practices and emerging trends. Respondents' answers were based on the 2004 calendar year.[1] Thirteen percent of the 819 survey respondents—more than double the 6% from the 2004 survey—reported that the total number of e-crimes (and network, system, or data intrusions) decreased from the previous year; 35% reported an increase in e-crimes; and 30% reported no change. Almost onethird (32%) of respondents experienced fewer than 10 e-crimes (versus the 25% reported in 2004), while the average number of e-crimes per respondent decreased to 86 (significantly less than 136 average reported in the 2004 survey). Respondents reported an average loss of $506,670 per organization due to e-crimes and a sum total loss of $150 million. While the average number of e-crimes decreased from 2003 to 2004, 68% of respondents reported at least one e-crime or intrusion committed against their organization in 2004; and 88% anticipated an increase in e-crime during 2005. More than half (53%) expected monetary losses to increase or remain the same. When asked what e-crimes were committed against their organizations in 2004, respondents cited virus or other malicious code as most prevalent (82%), with spyware (61%), phishing (57%), and illegal generation of spam e-mail (48%) falling close behind. Phishing jumped from 31% in the 2004 survey to 57%, the largest single percent increase of an e-crime year to year.