Chapter L
EU Tackles Cybercrime

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

ABSTRACT

The growing importance of information and communication infrastructure opens up new opportunities for criminal activities. The European Union has therefore taken a number of steps to fight harmful and illegal content on the Internet, protect intellectual property and personal data, promote electronic commerce and tighten up the security of transactions. However, in spite of the EU initiatives, many observers believe that cybercrime requires an international response that should include countries that are havens for cybercriminals.

INTRODUCTION

The European economy is moving from a predominantly industrial society to an information society. Communication networks and information systems are vital in the economic and societal development of the European Union (EU). The development and growth of information and communication technologies have been accompanied by an increase in criminal activities, which have been detrimental to the development of electronic commerce (e-commerce). Network and information security problems continue to grow as information flows freely across national borders. The Internet is increasingly used as a tool and medium by transnational organized crime, undermining user confidence, and generating substantial financial damage. Cognizant of the importance of computing networking and the need for secure communication networks and initiatives, the EU has adopted various instruments to combat criminal activity in the Internet. The following article provides a survey of current EU initiatives on combating cybercrime and an analysis

Copyright © 2008, IGI Global, distributing in print or electronic forms without written permission of IGI Global is prohibited.

of the council framework decision on attacks against information systems, which will be enforced in the EU in 2007.

BACKGROUND

The growing importance of information and communication infrastructure opens up new opportunities for criminal activities. Since the early '90s, the EU has taken steps to assess cyberthreats and the nature of cybercrime. The EU, therefore, has taken a number of steps to fight harmful and illegal content on the Internet; protect intellectual property and personal data; promote e-commerce; and tighten up the security of transactions. The action program on organized crime, adopted by the council (justice and home affairs) in May 1997 and endorsed by the Amsterdam European Council, called on the commission to carry out a study on computer-related crime.

In 1997, the European Commission commissioned a report to study the legal aspects of computer crime. The study (Sieber, 1998) was prepared under a contract with the European Commission. While this study did not focus specifically on cyber terrorism, it contributed greatly to the understanding of the vulnerability of information technologies to criminal activity. According to the study (known as the COMCRIME study), the various national laws have remarkable differences, uncertainties, or loopholes, especially with respect to the criminal law provision on infringements of privacy, hacking, trade-secret protection, and illegal content. On the international level, there was a lack of coordination among the various organizations, which risks the start of redundant programs. The report recommended that future measures against computer crime must be *international,* since different national strategies with the aim of preventing computer crime would create "data havens" or "computer crime havens," which, in turn, would lead to market restrictions and national barriers to the free flow of information and Europe-wide services (Sieber, 1998).

In October of 1999, the Tampere Summit of the European Council concluded that high-tech crime should be included in the efforts to agree on common definitions and sanctions. The following year, the European Council adopted a comprehensive eEurope Action Plan that highlighted the importance of network security and the fight against cybercrime.

The commission issued Com 2000 (890), which discussed the need for and possible forms of a comprehensive policy initiative in the context of the broader information society and freedom, security and justice objectives for improving the security of information infrastructures and combating cybercrime, in accordance with the commitment of the EU with respect to fundamental human rights. The communication addressed computer crime in its broadest sense as any crime involving the use of information technology. The terms "computer crime," "computer-related crime," "high-tech crime" and "cybercrime" share the same meaning in that they describe a) the use of information and communication networks that are free from geographical constraints and b) the circulation of intangible and volatile data. Whereas the computer-specific crimes require updates of the definitions of crimes in national criminal codes, the traditional crimes performed with the aid of computers call for improved cooperation and procedural measures.

These characteristics called for a review of existing measures to address illegal activities performed on or using these networks and systems. Other than a council decision on child pornography on the Internet and the framework decision, there are so far no EU legal instruments directly addressing computer-related crime, but there are a number of indirectly relevant legal instruments.

According to the communication, the main offenses covered by existing European and national legislation are:

1. **Privacy offenses:** Illegal collection, storage, modification, disclosure, or dissemination of personal data. Member states are clearly obliged by 95/46/EC to adopt all suitable measures to ensure the full implementation of the provisions of the directive, including sanctions to be imposed in case of infringements of the provisions of

6 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/tackles-cybercrime/7482

Related Content

Trust Enforcing and Trust Building, Different Technologies and Visions
Michele Tomaiuolo (2012). *International Journal of Cyber Warfare and Terrorism (pp. 49-66).*
www.irma-international.org/article/trust-enforcing-and-trust-building-different-technologies-and-visions/90840

State Terrorism and Its Impact on the Global Processes
Valeria Gonitashvili (2023). *Global Perspectives on the Psychology of Terrorism (pp. 136-159).*
www.irma-international.org/chapter/state-terrorism-and-its-impact-on-the-global-processes/314672

The Role of the (H)Ac(k)tivist
(2019). *Utilization of New Technologies in Global Terror: Emerging Research and Opportunities (pp. 76-96).*
www.irma-international.org/chapter/the-role-of-the-hacktivist/229241

A World without Islam
Maximiliano E. Korstanje (2012). *International Journal of Cyber Warfare and Terrorism (pp. 50-52).*
www.irma-international.org/article/world-without-islam/75765

A Comparative Analysis of the Cyberattacks Against Estonia, the United States, and Ukraine: Exemplifying the Evolution of Internet-Supported Warfare
Kenneth J. Boyte (2017). *International Journal of Cyber Warfare and Terrorism (pp. 54-69).*
www.irma-international.org/article/a-comparative-analysis-of-the-cyberattacks-against-estonia-the-united-states-and-ukraine-exemplifying-the-evolution-of-internet-supported-warfare/181793