IDEA GROUP PUBLISHING **ITB13045**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

This paper appears in the publication, *Digital Crim and Forensic Science in Cyberspace*
edited by Panagiotis Kanellis, Evangelos Kiountouzis, Nicholas Kolokotronis, and Drakoulis Martakos

Chapter XII

Law, Cyber Crime and Digital Forensics: Trailing Digital Suspects[1]

Andreas Mitrakas,
European Network and Information Security Agency, Greece

Damián Zaitch, Erasmus University, The Netherlands

Abstract

The steep increase of cyber crime has rendered digital forensics an area of paramount importance to keep cyber threats in check and invoke legal safety and security in electronic transactions. This chapter reviews certain legal aspects of forensic investigation, the overall legal framework in the EU and U.S. and additional self-regulatory measures that can be leveraged upon to investigate cyber crime in forensic investigations. This chapter claims that while full-scale harmonisation of forensic investigation processes across the EU and beyond is unlikely to happen in the foreseeable future, cross-border investigations can be greatly facilitated by initiatives aiming at mutual assistance arrangements based on a common understanding of threats and shared processes. Involving the users through self-regulation and accountability frameworks might also contribute to reducing risks in electronic communications that emanate from cyber criminal threats.

Introduction

Relying on information technology in transactions has led to the steep rise of criminal acts that are carried out through the use of Information and Communication Technologies (ICT) or target information technology resources for malicious purposes. Although information security measures strive to protect information systems users and service providers alike, electronic crime marks a growing trend. The opportunity to access vast interconnected information resources through open electronic networks multiplies exponentially the level of potential benefit that criminals can reap if they attack successfully information systems and their users. Cyber crime has already been subjected to regulation and is a matter of concern for public and private parties involved in electronic transactions. Forensic investigation of cyber crime emerges as a necessary link between evidence that is left behind at a crime scene and its potential use in criminal proceedings. Forensic investigations aim at following the trail that alleged criminals leave behind and connecting the various elements discovered with a view to obtaining an integrated view of the situation at hand.

The legal framework associated with forensic investigation nurtures concerns related to protecting fundamental rights such as privacy and data protection, data confidentiality, trade secrets, and intellectual property rights. Beyond the emerging legal framework voluntary frameworks for handling, retaining, and archiving systems and data set the stage for greater end user involvement in digital forensics. Methods and practices to conduct digital investigations are of particular importance especially in areas where rights might be at stake or sensitive information is risking disclosure. The approach to accessing and managing information is also critical for the admissibility of that information as evidence in a trial or other proceedings. Information security practices safeguard the quality and reliability of collected information. Additional attention must also be paid to cooperation across law enforcement agencies as well as the initiatives of the EU to counter cyber crime by safeguarding network and information security.

This chapter kicks off with an overview of digital forensics from a criminology viewpoint prior to reviewing some pertinent legal aspects. A criminological overview brings in the social and behavioural elements that are critical in assessing criminal acts. Pursuant to the criminological typology of cyber crime, some definitions and specific features of cyber crime, this chapter addresses the procedural framework to investigate cyber crime. This chapter also presents certain legal aspects of forensic evidence investigation in the EU and the U.S., the overall legal framework associated with information security safeguards and the institutional framework that can contribute to investigating and keeping cyber crime at bay. Finally some self-regulatory aspects are presented as well as some pertinent future trends.