Chapter X
Digital Forensics and the Chain of Custody to Counter Cybercrime

Andreas Mitrakas
European Network and Information Security Agency (ENISA), UK

Damián Zaitch
Erasmus University, The Netherlands

ABSTRACT

Targeting information technology resources has marked a growing trend for all sorts of reasons that include, profit making, causing damage, carrying out espionage, exploiting human beings etc. Although information security is used to protect information assets, electronic crime remains firmly on the rise. Computer forensics is the analysis of data processing equipment such as a data carrier, a network etc. to determine whether that equipment has been used for illegal or unauthorised purposes. Establishing the chain of custody through appropriate policy frameworks can be used in order to assess the quality of the collected data. Policy for forensics may address the practices of forensics agents and labs in investigating cybercrime. This chapter concludes that full-scale harmonisation of policies on criminal law and legal processes is likely to only happen at regional level (e.g. the EU) rather than at a global scale. Along with the assumption that safe havens where criminals operate from are not likely to be suppressed any time soon, leads to the conclusion that cyber-crime is here to stay for the long run in spite of the good efforts made to trail digital suspects through digital forensics.

INTRODUCTION

The growing dependence on information technology to carry out daily transactions has led to the steep rise of crime perpetrated by using Information and Communication Technologies (ICTs). Targeting information technology resources has also seen a growing trend for all sorts of reasons that potentially include, profit making, causing damage, carrying out espionage, exploiting human beings etc. Although information security is used to protect information asset electronic crime is on the rise. The opportunity to access vast interconnected information resources through open electronic networks increases the risk for users and potential benefit that criminals can reap if successful in attacking information systems. Regulating cybercrime has been challenging due to discrepancies across the board when it comes to cross border cybercrime definition and enforcement. Forensic investigation of cybercrime emerges as a necessary link between the hard evidence that can be leveraged upon from a crime scene and its potential use in criminal proceedings. Forensic investigations aim at following on the criminals' footsteps to reconstruct a crime scene and closely describe the various elements discovered with a view to obtaining an exact view of the crime scene at the time of the act. Forensics is essential in combating cybercrime.

The emerging legal framework and the voluntary frameworks for handling, retaining and archiving systems and data require some degree of preparation in order to ease up the collection and exploitation of data collected at a crime scene. 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 mostly in terms of integrity and authentication.

This chapter provides a typology of cybercrime from a criminological perspective that brings in the social and behavioural elements that are critical in assessing criminal acts. Thereafter this chapter reviews some pertinent procedural and legal aspects as well as the methodological framework to investigate cybercrime.

FRAMING THE DEBATE

Forensics or forensic science is the application of science to questions, which are of interest to the legal system. Computer forensics is the analysis of data processing equipment such as a data carrier, a network etc. to determine whether that equipment has been used for illegal or unauthorised purposes. Linking the equipment with its user can provide breakthroughs in the investigation process of an illegal act or a crime.

In spite of the criminological debate regarding concept and scope, most authors and policy makers interchangeably use concepts such as high-tech crime, digital crime, e-crime, computer-facilitated crime, cybercrime or computer-related crime as mere synonyms. In this chapter the term cybercrime is used to describe computer assisted crime. Additionally this chapter addresses aspects of illegal acts that do not necessarily have an interest from a penal law or a criminology point of view, they consist, nevertheless breaches that have to be dealt with.

Cybercrime involves attacking information systems or data for malicious purposes that often include a wide variety of crimes against persons, property or public interest. In these instances information systems are used to facilitate criminal activity. In other cases cyber criminals might directly target such information systems for the purpose of making profit, stealing secrets or damaging the interest of third parties. Cyber attacks have received substantial attention in view