1 Introduction

Wytske van der Wagen, Jan-Jaap Oerlemans & Marleen Weulen Kranenbarg*

1.1 Cybercrime as a new field in criminology

This book provides an overview of criminological research and relevant legal aspects of cybercrime for academic education and professional practice. In doing so, it is important to realise that criminological research into cybercrime has only really gained momentum in recent years and is still developing. Although the first academic publications date back to the beginning of the 1990s, we have seen a significant increase in qualitative and quantitative research in this area in recent years. More and more studies make use of statistically strong research methods, larger and more relevant research populations, innovative research methods, more in-depth qualitative research and data or method triangulation. We are seeing new concepts being introduced and applied in the theoretical field. Furthermore, the increasing interplay between the online and offline realm underscores the expanding influence of digitalisation across various domains within criminology, extending beyond dedicated research into cybercrime.

Cybercriminal behaviour is also developing rapidly, presenting both challenges and opportunities for research. Unlike many traditional forms of crime, studying cybercrime often demands a technical understanding of Information Technology (IT). This book offers such technical insights in a clear manner, using concrete examples in the description of the development of the internet and cybercrime (Chapter 2), in the analysis of the types of cyber-dependent and cyber-enabled crime (Chapter 3 and 4) and in the discussion of the challenges in cybercrime investigations (Chapter 9).

* Dr. W. van der Wagen is a criminologist specialised in cybercrime. Prof. Dr. J.J. Oerlemans is assistant professor in Criminal Law at the Institute of Criminal Law & Criminology at Leiden University. He is also endowed Professor of Intelligence and Law at Utrecht University. Dr. M. Weulen Kranenbarg is assistant professor in Criminology at the Department of Criminology of the Vrije Universiteit (VU) Amsterdam.

The general terminology, definitions, and categorisations of cybercrime are explained in Section 1.2. Section 1.3 presents the objectives of the textbook and Section 1.4 provides an outline of the entire book's structure.

1.2 What is cybercrime?

Terminology

Although 'cybercrime' is currently the most commonly used term when we talk about digital or online types of crime, various other terms have been used over the years. These include 'net crime' (Mann & Sutton, 1998), 'Internet crime' (Burden & Palmer, 2003; Jaishankar, 2011; Jewkes & Yar, 2010), 'hypercrime' (McGuire, 2008), 'virtual criminality' (Capeller, 2001; Grabosky, 2001), 'high-tech crime' (van der Hulst & Neve, 2008), 'computer crime' (Casey, 2011) and 'technocrime' (Steinmetz, 2015a; Steinmetz & Nobles, 2017). In this book, we use the term *cybercrime*, because it is most frequently used. We use it as an umbrella term covering all types of crime in the cyber domain.

Definition

As cybercrime covers a wide range of offences, it makes it a difficult phenomenon to define. Many definitions are therefore quite broad and mainly emphasise the role of IT in committing crimes. Yar (2013), for example, provides the following definition: "A range of illicit activities whose 'common denominator' is the central role played by networks of ICT in their commission" (p. 9). Gordon and Ford (2006) speak of: "Any crime that is facilitated or committed using a computer, network, or hardware device" (p. 14). Thomas and Loader's (2000) definition closely resembles Yar's (2013), but it extends to encompass non-criminalised activities as well. According to Thomas and Loader, cybercrime encompasses "computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks" (p. 3). While these definitions are comprehensive, our focus in this book primarily revolves around criminalised behaviour and underscores the pivotal role of IT in these offenses. Therefore, in this book we use the following definition:

> Cybercrime includes all criminal conduct in which IT systems are essential in the execution of the offence.

Classification

In the criminological literature we can find various classifications of cyber offences. We use a classification that distinguishes two main categories of cybercrime: 'cyber-dependent crime' and 'cyber-enabled crime'.[1] The former refers to new offences that did not exist before the internet and in which IT is both the target and the means (e.g. hacking, distributed denial-of-service (ddos) attacks and the distribution of malware). The latter refers to traditional crimes that are committed by means of IT and where IT is used in the execution of the crime (e.g. cyberstalking, grooming and internet fraud).

Several other terms are also used to describe the dichotomy of cyber-dependent and cyber-enabled crime. Some researchers refer to these categories as 'computer-focused' versus 'computer-enabled crime' (Furnell, 2002) or 'cyber-focused' versus 'cyber-enabled crime' (McGuire & Dowling, 2013a, 2013b). This dichotomy primarily focusses on the target, whether that target is a computer system or not. However, it can also be viewed as a continuum, ranging from crimes heavily reliant on technical aspects at one end to those predominantly driven by human factors at the other (Gordon & Ford, 2006). In addition, a perpetrator may also commit a combination of cyber-dependent and cyber-enabled crime (also called a 'chain of crimes'), for example, when nude photos are stolen from a smartphone through hacking and then used in digital extortion (called 'sextortion'). Given the increasingly intertwined nature of the online and offline world, it is however important to emphasise that technology plays a role in many crimes, particularly in facilitating communication among offenders. Hence, for a crime to be considered a cyber-enabled crime the use of IT must be essential. This means that the crime would be substantially different if no computer system was used. In section 2.3, we discuss a number of different ways in which computer systems have substantially changed crime.

Although the classification of cyber-dependent versus cyber-enabled crime is central to this book, it is important to mention a number of other commonly used classifications that distinguish three or more groups of crimes. All the

[1] This classification is loosely based on the classification made by Wall in his groundbreaking book about cybercrime in 2001 (Wall, 2001). However, the classification in this book is without the category of 'cyber-assisted crime'. We view the category of cyber-assisted crime simply as crimes in which the internet plays a role as a medium or environment and in which digital evidence may play a role, which is almost every crime nowadays.

way back in 1976, Parker developed a three-part classification in which the computer is regarded as an (a) object, (b) instrument or (c) environment for crime. In the case of the computer as an *object*, the offender aims to influence or affect the data stored in computers, including programmes. In the case of the computer as an *instrument*, the offender manipulates a computer system in order to commit a (traditional) crime. In the case of the computer as the *environment* of the criminal act, the computer system is part of a broader environment in which the criminal act is committed and may provide important evidence.

Another classification that has frequently been used in criminology, especially in the past, is the one proposed by Wall (2007a). He describes three successive generations of cybercrime, based on the degree to which the crime is new or different from traditional crime. The first generation involves crimes in which the computer is used to commit traditional crimes. These crimes are in fact 'old', but take place with new technologies (such as cyberstalking, hate crimes and [small-scale] cyberfraud). The second generation includes traditional forms of crime, which now have a more global character due to digitalisation. They are old in terms of the basic crime itself, but new in terms of the instruments used and their scope. Examples are large-scale fraud or online fraud schemes targeting multiple victims around the globe simultaneously, or the large scale and worldwide distribution of online Child Sexual Abuse Material (CSAM). In these crimes, technology acts as a 'force multiplier', a term that refers to the principle that one single person can commit a crime on a massive scale (Wall, 2007a; Yar, 2005a, see also Section 2.3.2). The third generation refers to so-called 'true' cybercrimes, crimes that are entirely generated by network technology. They have a distributed and automated character, are not limited by time and space and would disappear completely if the internet ceased to exist. In these crimes, technology is not only a force multiplier, but also the crime target, just like cyber-dependent crimes as discussed earlier. Wall also includes crimes in this generation that take place entirely in virtual worlds, such as cyber rape or cyber theft (see further Section 2.2.6). Wall's (2007a) classification thus places more emphasis on how technological developments have influenced the various types of cybercrime (see Chapter 2 for an overview of how technology and cybercrime have developed globally through time). For a detailed inventory of all definitions, typologies and taxonomies used in the literature, we refer to the overview study by Phillips et al. (2022).

1.3 Purpose of this book

Research into cybercrime significantly increased in recent years. As cybercrime has become a major issue in various countries around the world and has become an important focus for law enforcement agencies alike, cybercrime has established an important place on the criminological research agenda. This resulted in numerous academic articles, books and other publications on cybercrime. There is also increasing attention for cybercrime at conferences such as the European Society of Criminology Conference (ESC) and the American Society of Criminology Conference (ASC), visible in the number of presentations and sessions that are organised. In addition, various international networks of researchers have emerged such as the 'Annual Conference on the Human Factor in Cybercrime',[2] which started in 2018 (with an annual conference as well), the 'Division of Cybercrime' of the 'American Society of Criminology',[3] and the 'Working Group on Cybercrime' of the 'European Society of Criminology'.[4] Finally, there is a never-ending stream of news items and reports from cybersecurity companies that constantly remind us of the impact that cybercrime has on our society.

A textbook on the essentials of cybercrime is in our view necessary in order to bring together knowledge about cybercrime in a conveniently arranged manner. That is why in 2020 we published our (Dutch) textbook *Basisboek Cybercriminaliteit* (Van der Wagen et al., 2020), in which all the essential knowledge about cybercrime was provided. As some universities expressed the desire for an English version of the book, we decided in 2021 to move forward with a translation. However, the book is not a direct translation of the Dutch version. It has a more international orientation. Given the enormous interest in the books and the fact that we would like to keep the knowledge on cybercrime up-to-date as much as possible, we decided to publish a second edition of both the Dutch and English book in 2024. In this edition, all chapters have been thoroughly updated, expanded, renewed and/or revised. Section 1.4 provides a detailed overview of the structure of this edition.

Our expectation is that by studying this book, readers will gain essential knowledge about cybercrime. We understand that not all aspects, offences, and studies related to cybercrime are covered. As authors and editors, we have made choices based on years of experience in researching cybercrime and

[2] See https://www.hfc-conference.com/.

[3] See https://asc41.org/divisions/dc/.

[4] See cybercrimeworkinggroup.com.