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 been in full development for only a few years. Although the first 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, and data or method triangulation. We are also seeing new concepts being introduced and applied in the theoretical field.

Cybercrime as a criminal domain is also developing rapidly, and therefore it is a challenging and fascinating field of research. Unlike most traditional forms of crime, cybercrime can be very technical in nature. Therefore, a certain level of understanding of Information Communication Technology (ICT) is required to fathom the subject matter. This book provides this technical knowledge in a clear manner and on the basis of concrete examples in the description of the development of the internet and cybercrime (Chapter 2), in the analysis of the types of cybercrime (Chapter 3) and in the discussion of the challenges in cybercrime investigations (Chapter 8).

Before discussing the structure of the entire book, the applied definition and categorisation of cybercrime are explained in Section 1.2. Section 1.3 presents

* Dr. W. van der Wagen is assistant professor in criminology at the Erasmus School of Law (Erasmus University Rotterdam). Prof. dr. J.J. Oerlemans is an endowed professor of intelligence and law at the Willem Pompe Institute for Criminal Law and the Montaigne Centre for the Rule of Law and Justice of Utrecht University. Dr. M. Weulen Kranenbarg is assistant professor in criminology at the School of Criminology of the Vrije Universiteit (VU) Amsterdam.

the objectives of the study book and Section 1.4 provides an outline of the book's structure.

1.2 What is cybercrime?[1]

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 cybercrime.

Definition

Because 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 ICT 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 is very similar, but it also includes non-criminalised activities. This definition reads: "Computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks" (p. 3). These definitions are all quite broad and general. In this book, we focus mainly on criminalised behaviour and we want to emphasise the role of ICT in these offences. Therefore, in this book we use the following definition, which is based on the above definition by Yar (2013):

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

1 This paragraph is partly based on Chapter 1 of the first author's doctoral thesis (Van der Wagen, 2018a).

Classification

In the criminological literature we can find various classifications to distinguish cyber offences. We use a classification that distinguished two main categories of cybercrime: 'cyber-dependent crime' and 'cyber-enabled crime'.[2] The former refers to new offences that did not exist before the internet and in which ICT 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 ICT and where ICT is used in the execution of the crime (e.g. cyberstalking, grooming and internet fraud).

The dichotomy between cyber-dependent and cyber-enabled crime is also often used with different terms in other studies. There they speak of 'computer-focused' versus 'computer-enabled crime' (Furnell, 2002) or 'cyber-focused' (or cyber-dependent) versus 'cyber-enabled crime' (McGuire & Dowling, 2013a, 2013b). The dichotomy is, as can be seen, primarily based on the target (ICT or not). However, the dichotomy can also be seen as a continuum of crime that is very technical in nature at one end, and crime that is still very much human-related at the other end (Gordon & Ford, 2006). In addition, a perpetrator may also commit a combination of cyber-dependent and cyber-enabled crime, for example, when nude photos are stolen through hacking from a smartphone and then used in digital extortion (called 'sextortion').

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

2 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.

of a broader environment in which the criminal act is committed and may provide important evidence.

Another classification that has been often 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. 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 on which child pornography is distributed worldwide. In these crimes, technology acts as a 'force multiplier', which is 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 'real' 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 target of the crimes, just like cyber-focused 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).

1.3 Objective of the book

Research into cybercrime greatly increased in recent years. As cybercrime has become a major crime 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 scientific 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 (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',[3] which started in 2018 (with an annual conference as well), the 'International Interdisciplinary Research Consortium on Cybercrime'[4] and the 'Working Group on Cybercrime' of the 'European Society of Criminology'.[5] 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 study book about 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) studybook 'Basisboek Cybercriminaliteit' (van der Wagen, Oerlemans, & Weulen Kranenbarg, 2020), in which all the necessary basic knowledge about cybercrime was provided. As some universities expressed the desire for an English version of the book, we decided to move forward with a translation. The current book is however not a literal translation. It is more internationally oriented, especially when it comes to legislation, it includes the most recent studies, and it also provides an entirely new chapter on organised cybercrime (Chapter 5). Like the Dutch version of our book, it aims to provide essential knowledge of various facets of cybercrime. We are aware that not all offences and available studies on cybercrime are mentioned in the book. As authors and editors, we have made choices in what we believe is most important for students and professionals, based on the years of experience we have in researching cybercrime. By mentioning some discussion questions at the end of the chapters, we indicate relevant issues that may be suitable for discussion or interesting for further research. Also, at the end of each chapter an overview is given of the most important key concepts that have been dealt with. We encourage lecturers to provide additional material (e.g. scientific articles cited in this book) for a possible deepening of parts of the book. Due to the rapid developments in the area of cybercrime, it is important that lecturers are alert to outdated facts, new studies and new criminal offences or investigation methods. Students can also play an active role in this, by asking themselves after each chapter how the material discussed can be applied to recent technological developments.

3 See rechten.vu.nl/conferencecybercrime.
4 See cj.msu.edu/iircc/iircc.html.
5 See cybercrimeworkingroup.com.

Finally, we discuss in great detail the advantages and disadvantages of various research methods for studying cybercrime (Chapter 2), so that students and future researchers can take this into account when conducting scientific research and when interpreting the results in cybercrime research. We are convinced that the continuous digitalisation of society and crime calls for more research into cybercrime and a continuous development of the methods and theories used in this area. We hope that the readers of this book will acquire the necessary basic knowledge about cybercrime and see how fascinating this phenomenon is.

1.4 Structure of the book

This study book is structured as follows. Chapter 2 offers an overview of the historical developments of cybercrime, developments within cyber-criminology, and a theoretical and methodological perspective on cybercrime. Chapter 3 offers an overview of the various types and the most important criminal offences relating to cybercrime. Chapter 4 discusses developments, characteristics and factors that play a role in cybercrime offending. Chapter 5 provides insights in various aspects of organised cybercrime, including knowledge about the composition and structure of criminal groups and networks. Chapter 6 discusses the development of cybercrime victimisation and the factors that are associated with it. Chapter 7 discusses the extent to which traditional criminological theories can be applied to cybercrime and discusses new (cyber) criminological concepts. It can be regarded as the theoretical criminological perspective that is needed to explain the information from Chapters 4, 5 and 6 on cyber offending and victimisation. Chapter 8 is about the investigation process in cybercrime cases and the regulation of the investigation methods used. The book concludes with Chapter 9 with a discussion of interventions aimed at the offenders of cybercrime.

Finally, when reading the book, it is important to bear in mind that most chapters focus on both cyber-dependent crime and cyber-enabled crime (Chapters 2, 3, 6, 7 and 8), but that some chapters concentrate on cyber-dependent crimes only (Chapters 4, 5 and 9).