Preface

In the opinion of some commentators, crime has always been with us and computers are simply another tool criminals use to commit their offences. Accordingly, in one of the first books to place computers and law in the proper context, Colin Tapper asks the rhetorical question why there is "any more need for a book on the law of computers than there is for on the law of typewriters or tuning forks" (van der Merwe 2008, p. 61).

Tapper's answer boils down to the fact that computers were playing an increasingly important role in the community, that they were qualitatively different from anything else that had come before, and that traditional legal principles were inadequate to deal with the legal problems caused by computers (Ibid). Well into the twenty–first century these arguments seem more valid than ever. Not only has "the computer" been expanded into a wide-ranging and dynamic new concept called "information and telecommunications technology" (ICT), but the law is still desperately trying to keep up with this rapidly moving target (Ibid).

In the field of fraud by computer manipulation, many criminal law systems "de lege lata" face considerable difficulties in applying their traditional criminal provisions (Sieber 1998, Online). The statutory definitions of theft, larceny, and embezzlement in many legal systems are not applicable if the perpetrator appropriates deposit money; in many countries these provisions also cause difficulties as far as manipulations of cash dispensers are concerned (Ibid). The statutory definitions of fraud in many legal systems demand that a person be deceived. They cannot be used when a computer is "cheated" (Ibid).

At the same time that society is becoming more fragile, potential threats are expanding, diversifying, and becoming more opaque. The capability to launch cyberattacks that can exploit these strategic vulnerabilities is "shifting to the edge," that is, technology is empowering networked groups and individuals to directly threaten nation state security (and, thus, global stability) by putting critical infrastructure at risk (Brown et al. 2009, p. 671). Examples include:

- The "Millennium Bug" or Y2K program of 1997–1999, which led to a complete inventory of computing inside large organizations, often for the first time since the deployment of the enterprise Personal Computer (PC) in the mid-1980s;
- Denial of Service (DoS) attacks, beginning in 2001 against Yahoo! and eBay;
- Business continuity planning in the wake of the attacks in September 11, 2001;
- Corporate responses to the increasing financial returns for attackers (for example the growth of "phishing" and the 2004–2005 cyber-extortion cases against gambling websites);
- Cyberattacks against Estonia's government websites, 2007;
- 2010 FIFA World Cup Fraud;
- "Hacktivisit" supporters of Julian Assange allegedly shutting down MasterCard website in December 2010;
- U.S. defense firm Lockheed Martin struck by cyberattack in May 2011.

Intended Audience and Methodological Orientation

The book's main academic reference point is the intersection between law and criminology, particularly as it relates to the "law in action." Many harmful internet behaviors that raise public concern do not necessarily fall neatly within the criminal or civil codes. Furthermore, how they are currently resolved is framed increasingly by the broader discourse of public safety, as well as specific law enforcement debates. The book's intended audiences are advanced undergraduates and graduate students as well the various professional communities involved in cybercrime-related policy-making or practice.

This book contains a discussion about cybercrimes and the management issues they raise. The narrative is constructed from a grounded analysis of events and draws upon a range of different sources, as the distributed (as opposed to centralized) organization of the Internet creates multiple flows of often conflicting information about cybercrime offending and victimization. Networked information has the tendency to flow quite freely in all directions and so evade the editorial verification and control of dissemination which characterized previous media ages. Some of these information sources are the product of impartial and reliable news reporting, others are not. The latter may be the product of vested interest, or the results of academic research or surveys conducted by the many governmental and nongovernmental agencies that have an interest in most things "cyber".

Whenever possible, original and independent sources of information have been sought to ensure the reliability of information and in order to either (i) confirm a particular trend in two or more independent datasets or (ii) record the occurrence of an event. Adopting such an approach has helped to counter polemical accounts. Particular care was taken to avoid following purely sensationalized news streams, where one article reporting a sensational news event tends to spawn a chain of others.

The resulting analysis therefore takes a multidisciplinary approach to respect the many voices of crime. The digital realist perspective adopted here is not, however, to be confused with the artistic theory of pseudo-realism which carries the same name, or indeed, debates about left-realism. Rather, it originates in the work of many scholars who have been adapted here to contextualize cybercrime. Essentially, it is a multiple discourse approach which recognizes that cybercrime, like ordinary crime, is a form of behavior that is mediated by technology but also by social and legal values and economic drivers. The interrelation between these four influences not only shapes the digital architecture of criminal opportunity, but also provides some directions for resolving the same harms.

What follows, then, is a systematic enquiry based on available knowledge, literature, and research findings. It is also informed by my own research projects into cybercrime and cyber law conducted between 2003 and 2011.

What Is Covered?

This book is divided into five parts, each covering specific topics relating to cybercrime: What follows is a brief summary:

Part I: Fundamentals of Cybercrime
This part begins with an overview of cybercrime, the difference between cybercrime and similar offences, and the scale of the problem in the US, the UK, and the Middle East. This will be followed by a case study of several cybercriminals, as well as an illustration of the major challenges faced in fighting against this threat. The section concludes with an in-depth explanation of the future of Internet crime and punishment.

Part II: Computer System as Target
Part II of the book addresses the topic of computer hacking, by first covering the criminal statutes aimed at protecting computers in the US and the UK, and thereafter exploring types of malicious code, and the threats posed by viruses, worms, and Trojan horses. It concludes with an analysis of current threats and legislative approaches in the US, and the Council of Europe Convention on Cybercrime.

Part III: Computer System as Tool
Part III explains how the Internet is used as a tool and medium by cybercriminals. This includes the problem of phishing and the use of stolen financial information by phishers. The final chapter covers sexual harassment, providing readers with case studies to illustrate the prevalence of sexual harassment in cyberspace, enforcement problems, and the regulation of this threat in the US and the UK.

Part IV: Content—Related Offences
Part IV focuses on the role of the Internet in promoting child sexual abuse. This includes production of pornographic content, distribution and sharing, and the consumption of pornographic content. Criminal offences against children such as cybering, grooming, age play, and exposure to obscenity are also covered. The section ends with some strategies to minimize risks to youth when they access the Internet.

Part V: Privacy, Security, and Crime Control
Part V seeks to explore and analyze anonymity in cyberspace. It shows that the balance between privacy of Internet users and security of nations can be achieved. Furthermore, it focuses how anonymity can be achieved on the Internet and why it is an essential tool for free speech. This section will also describe national and regional strategies in Europe to fight against cybercrime. This section covers the Nigerian 419 scam, the operation of the scheme, the nature and extent of the problem, and an evaluation of the current situation in Nigeria.

Mohamed Chawki
International Association of Cybercrime
Prevention (AILCC)
Paris
France

Ashraf Darwish
Mohammad Ayoub Khan
Sapna Tyagi

References

I. Brown, L. Edwards, C. Marsden, in *Information Security and Cybercrime*, ed. by L. Edwards, C. Waelde. Law and the Internet (Hart, Oxford, 2009)
U. Sieber et al., *The Legal Aspects of Computer Crime and Security: A Comparative Analysis with Suggestions for Future International Action* (Elsevier, New York, 1998)
D. van der Merwe et al., *Information and Communications Technology Law* (LexisNexis, Durban, 2008)

http://www.springer.com/978-3-319-15149-6

Cybercrime, Digital Forensics and Jurisdiction
Chawki, M.; Darwish, A.; Khan, M.A.; Tyagi, S.
2015, XVIII, 145 p., Hardcover
ISBN: 978-3-319-15149-6