Book Review:

Jonathan Clough, *Principles of Cybercrime*, 2nd ed (Cambridge: Cambridge University Press, 2015)

Christopher D. Ram[*]

The past decade has seen an enormous explosion of scholarship on the subject of cybercrime, as technologies and offenders pose new challenges and law enforcement, government and academic experts struggle to keep up. The new, second edition of Professor Jonathan Clough's book occupies a fairly substantial, but specific niche in this increasingly diverse and complex landscape. *Principles of Cybercrime*[1] contains only a cursory review of the history and criminology of cybercrime, it does not deal at all with IT security, investigative or enforcement matters, and discussion of cybercrime as a global issue is limited to brief discussions of the 2001 *Budapest Convention*[2] and extensions of domestic law jurisdiction. Readers seeking any sort of detailed information in these areas or a comprehensive resource covering the entire field should probably look elsewhere.

What the book does deal with is the classification and description of cybercrime offences as matters of substantive criminal law, based on five primary, common-law sources: the offences and case law of Australia, Canada, New Zealand, the United Kingdom and the United States of America, as well as provisions of the *Budapest Convention*, which all five have implemented (Canada after the book went to press). Within this scope it is an excellent, well-organized, accessible, and to the extent possible in such rapidly-evolving areas, comprehensive reference source.

"Cybercrime" is a term of art, not of law or forensics, and issues of definition and typology have always been a challenge. *Principles of Cybercrime* updates earlier distinctions based on "computer crime" and "computer-related crime", discussing crimes as "cyber-dependent", "cyber-enabled", and "computer-supported" and follows a typology that approximates the *Budapest Convention* and laws of the five countries considered. It solves the typological problem by commencing each segment with a brief criminological overview of relevant technologies and their misuse. This general description is then followed by a comparative review of legislative case law—including, for Australia and the United States, relevant state and territorial laws and cases. This format greatly

---

[*] LL.B., LL.M. Counsel, Criminal Law Policy Section, Justice Canada.

[1] Jonathan Clough, *Principles of Cybercrime*, 2nd ed (Cambridge: Cambridge University Press, 2015).

[2] Council of Europe Convention on Cybercrime, C.E.T.S. No. 185, Can. T.S. 2015/18 (2001).

facilitates comparison of offences and case law, saving many hours of comparative law research. This makes it a useful primary tool for academics, students and policy analysts, and the comparative and thematic access to case law would also greatly assist prosecutors and other litigators. It is sufficiently accessible to provide relatively easy access to cybercrime law for non-lawyers.

The original distinction between the use of computers as instruments for crime and the targeting of computer systems and data as a new form of crime led to coverage of some content, such as the prevalence of cybercrime and background and historical information about legislation, in Part II of the first edition, "The Computer as Target".[3] The same pattern was followed in the revision, and this has to some extent been overtaken by changes in crime itself. Most current discussions of prevalence either focus on specific offences or cybercrime as a whole and not just what the book labels "cyber-dependent" crimes where computers or data are the targets. The original distinction between the two basic types has evolved into a much more complex landscape insofar as offending and occurrence rates are concerned. Overviews of legislation, also discussed in chapter 2, are also no longer limited to computer-specific offences, but have spilled over into other areas such as laws dealing with privacy and electronic surveillance. The use of computers and networks has also transformed traditional areas such as the suppression of criminal harassment and child pornography. Those are the subjects of specific chapters, but the same transformations have also influenced the general legislative environment. Much of what is said in chapter 2 now applies to cybercrime in general, not just cyber-dependent crime, and it would be useful if this was expanded and moved to the introductory or general part of the book in the next revision.

The same is true for content in several other chapters, which by virtue of shifting crime patterns could now be considered as having more general application. The meaning of terms such as "computer" and "data" were originally specific to cyber-dependent crimes, but in Canada most of the cases considering these terms are now computer-enabled offences such as the production or dissemination of child-pornography. That may to some degree depend on the relative priorities given different crimes by law enforcement and prosecution officials, but the vast majority of cases everywhere appear now to be computer-enabled as opposed to computer-dependent in nature, and this will no doubt influence how law-makers and judges define key terms. What is a "computer" has obviously been transformed in a world filled with "smart phones" and computer chips in everything from automobiles to toasters. Moving those to the introductory part of the book would also assist in linking technological evolution and technology-neutrality to the challenges legislatures now face in ensuring that every new offender innovation does not trigger a need for statutory amendments.

---

[3] Jonathan Clough, *Principles of Cybercrime* (Cambridge: Cambridge University Press, 2010).

The discussion of prevalence sets out what information is known in a fairly chaotic manner, not through any fault of the author but because the information itself is chaotic. The book faithfully reports what information is known, but the data are from a small number of sources in a small number of developed countries, and some discussion of why this is so and whether or not the picture they paint can safely be extrapolated would have been useful. There also appear to be huge gaps between rates of offending and rates of prosecution and this might have been pointed out and some discussion of whether this is a statistical artefact or a real gap, and if so, why, would also have increased the value of the information that is provided. Questions of reporting and measuring cybercrime could be (and in some cases are) complete books in their own right, but as a criminologist I would have liked to see more discussion and analysis both of what the data available actually mean, the extent to which they can be relied upon and why they are not more complete.

The main reason that rigid typologies of cybercrime are problematic is the constant convergence of technologies and evolution of cybercrime itself. The book avoids problems of overlap (and rapid obsolescence) by using general descriptions, but it could benefit from more detailed discussion of some of these issues and cross-referencing in the text and footnotes. One such area is the convergence of telecommunications and data-transfer (which is discussed in chapter 6), more general legislation and offences relating to electronic surveillance as an invasion of privacy, and the specific intrusions on privacy and other protected interests raised by criminal harassment and voyeurism (chapters 12 and 13). Some of the differences between the countries considered have less to do with basic policy than the choice of which pre-digital legislative scheme was expanded to cover specific cybercrime problems.

Aside from updating the case law, most of the content revised from the first edition relates to changes in the scope of actual cybercrime in areas such as the use of malware (chapter 2) and criminal harassment (chapter 12). The rapid changes in these areas are no doubt among the reasons a second edition after only five years was thought to be warranted. One of the book's strongest points is the format of the various substantive chapters, which commence with a factual review of what offenders actually do and how various types of malware actually work. Here the factual summaries are excellent, providing a sufficient overview to allow for an informed basis of what legislatures have enacted and courts have decided as a result, without being overly technical or getting bogged down in detail. The book focuses on law and it is not intended to be a manual for IT professionals any more than for cyber-criminologists, but as noted both technical and legal discussions are clearly set out in language that should be accessible to all, making it a useful reference on cybercrime law for non-legal professionals.

The global nature of cybercrime does make the specific focus on offences in common law systems a drawback in considering broader issues. By and large these are beyond the scope of the book, but the chapter on jurisdiction, which relies primarily on domestic enactments and the *Budapest Convention*, would be

improved by greater reliance on public international law sources. This is also a chapter that could usefully be expanded and moved to the introductory part of the book. There is no significant difference between extensions of territorial jurisdiction over cyber-dependent offences such as hacking or the propagation of malware, and over cyber-enabled crimes such as transnational fraud or the dissemination of child pornography.

The author wisely avoids law enforcement and investigative issues as beyond the scope of the book, but some discussion of enforcement issues is needed in any examination which considers extraterritoriality of enforcement jurisdiction. Prof. Clough correctly points out that *in personam* enforcement can only be done by the country which has custody of the accused and provides a useful overview of extradition issues, but does not address the other key aspect of enforcement jurisdiction: the issues raised by any sort of extraterritorial or cross-border searches or data-interceptions. These are subject to the customary law principles of territoriality and sovereign independence, such that any sort of intrusive investigation can only be done with the consent of the State in whose territory the target infrastructure, devices or data are located. Confusing prescriptive and adjudicative jurisdiction, which may deal with extraterritorial elements in most cases, and enforcement jurisdiction, which requires consent, is a common mistake for non-lawyers, and to the extent the book is intended as a general reference work for this audience it would have been very helpful to have made this clearer.

As noted, *Principles of Cybercrime* seeks only to examine and compare the laws of five common law countries. Adding many civil law countries would make the comparative structure of the book (and no doubt its length) unmanageable, but a basic overview of non-common-law approaches would also add value, especially as most States Parties to the *Budapest Convention* have civil law systems.

But these are for the most part quibbles about what the book is not. What it is, is an excellent, detailed and comprehensive reference work on cybercrime as it presently stands in the laws of the leading common law countries. For those seeking easy access and insight within that scope it is highly recommended.