The Denning Law Journal 2014 Vol 26 pp 301-304

BOOK REVIEW

CYBER CRIME

Cyber Crime & Warfare, Peter Warren and Michael Streeter, Hodder & Stoughton, London, UK, 2013 ISBN 9781444189988 Price £8.99 pb

Cybercrime – The Psychology of Online Offenders, Grainne Kirwan and Andrew Power, Cambridge University Press, Cambridge, UK, 2013 ISBN 978-0521180214 Price £23.99 pb

Jocelynne A Scutt[*]

None of these four authors is a lawyer. Yet both books are strong contributors to the field of cybercrime and essential reading for lawyers – as well as forensic psychologists, journalists, filmmakers, creative and information technologists, and historians interested in this burgeoning field. The historical accounts in both of the on-going development of cybercrime are particularly rewarding for lawyers from a common law background: they recount well the ingenuity of the criminal mind and the way common law can adapt to new developments, whilst pinpointing common law adaptability limitations spurring parliamentary intervention. Simultaneously, the books encapsulate well the excitement generated by the rise of the computer and the internet, the invention of the World Wide Web, and the escalating growth of social media.

Cyber Crime & Warfare is written by two journalists with a wealth of complementary expertise, the book being blessed with an engaging style which makes it easily read: I did this in one sitting. Directed at the general reader and specialists from a range of disciplines, eleven chapters cover ‘The nature of cyber crime’, through ‘The history of hacking’, ‘The rise of the internet and virus threat’ and cyber espionage, identity theft, spam, botnets and ‘Cyber warfare and the information war’. Chapters also describe the profiles of cyber criminals and ‘Policing cyber space’ as well as the troubling engagement of the internet and the vulnerable: ‘Targeting children’. The book ends with a chapter on ‘Future technology ...’ and ‘100 ideas’ for exploration of the subject in great depth. The 100 list includes websites, historical and

[*] The Hon Dr Jocelynne A Scutt, Barrister & Human Rights Lawyer, Visiting Fellow, Lucy Cavendish College, University of Cambridge, Visiting Professor, University of Buckingham.

contemporary locations for pursuing hacking history, annual conferences, films, non-fiction books, cybercrime fighting organisations, destructive computer viruses and worms, famous hackers or cyber criminals, hackers-in-fiction (including Stieg Larsson's Lisbeth Salander and Michael Crichton's Dennis Nedry of *Jurassic Park*) and 'Five spectacular hacks', (the 77m accounts compromised through the 2011 hacking of the Sony PlayStation Network being one) plus 'Ten key milestones in the history of cybercrime' .

Cybercrime sets out consciously to be a graduate and undergraduate text book, the first chapters introducing key concepts (forensic psychology and cybercrimes) and offences specific to computer hacking and malware, followed by chapters covering crimes facilitated by computer technology or becoming more prevalent with its advent, including copyright infringement, identity theft, fraud, terrorism, bullying, stalking, child pornography and child sexual exploitation. The final chapter addresses crime committed in virtual worlds. Each chapter commences with case studies anticipating what is to follow and introducing readers to computer and internet crimes of varying types, their impact on victims and survivors, (possible) consequences for perpetrators and, sometimes, perpetrators' excuses, explanations or rationalisations. A chapter overview and conclusion sandwich the substantive content which is fashioned into sections followed by short summaries or activities students can undertake to ensure they have a good grasp of the material. Additional assistance to students is provided through model essay questions and lists of additional reading at each chapter conclusion. This format makes the student audience objective clear, yet does not detract from the interest or value to those pursuing the field for reasons other than exam-taking. That the authors work in the Dublin Institute of Art, Design and Technology (IADT) ensures they know their subject well and are adept combining their respective skills, qualifications and expertise to ensure a captive audience: Grainne Kirwan is a psychology lecturer, her doctoral thesis researching ethics, motives and interpersonal relationships of hackers, whilst as IADT Head of the Faculty of Film, Art and Creative Technologies, Andrew Power comes with 18 years ICT industrial experience and a doctorate researching active citizenship linkages through social networking.

For criminal law teachers, particularly, ***Cybercrime*** and ***Cyber Crime & Warfare*** provide opportunities for incorporating into traditional criminal law teaching examples and perspectives on existing criminal fields that can connect well with new generations of law students. Tort teachers could also benefit, adapting criminal law scenarios to their field. As the books raise ethical questions, too, their relevance to law in contemporary times and the teaching of law students who use computers – including iPhones and other electronic devices - and the internet as a matter of course is self-evident.

The books are timely, particularly with recent high profile trials having brought hacking to the fore. Initial naivety and lack of awareness about the intrusions and the capacity of journalists to engage in them have generated, at times, daily coverage of angry, upset and sometimes traumatised victims and survivors. Yet this could be considered surprising in light of the longevity of this practice. Hacking originated in the 1950s, when academics at MIT and other science universities created and employed these skills, generating advances in information technology now underpinning the far reaching positive uses of computers and the internet today. Warren & Streeter point out that thirty years ago the prosecution of Robert Schifreen and Stephen Gold under the 1981 Forgery and Counterfeiting Act failed when, on appeal, the court ruled that charges of forgery, theft and criminal damage had no applicability to hacking into the mailbox of Philip Windsor (husband of the British monarch). This prosecutorial failure generated the Computer Misuse Act 1990 (UK), reflecting the US Computer Fraud and Abuse Act of 1984.

Both books discuss at some length hacking as a socio-criminal phenomenon. Kirwan and Power provide the most comprehensive coverage, devoting an entire chapter to 'Hackers' and debating varying definitions which attest to the fluid or variable assessment of this activity. Confirming, however, that traditional ways of looking at crime, criminality and criminals persist, the hacking world is populated by white hat and black hat hackers – as well as a new category, grey hat hackers. Those in the 'white' camp engage in hacking activity which is formally criminal, however, they do so for 'good' reasons – to discover flaws in IT systems and failures of security so as to alert system owners and, on occasion, correct these failures and flaws. 'Black hats' engage in the same hacking practices – yet use the information gained for nefarious purposes: syphoning off large monetary sums being a principal pursuit. Those under the 'grey' headgear hack to uncover flaws and failures – then alert the subject companies or governments, demanding payment for information that will counter the problems, or offering their expertise to correct them – at a price.

The difficulties of policing nefarious activities online, the international nature of this criminal activity – adding not only to policing difficulties but to framing effective legislation in the first instance – are canvassed well – more briefly in ***Cyber Crime***, more extensively in ***Cybercrime & Warfare***, yet both providing useful insights. Cooperation between crime agencies on an international basis is a positive development leading to multiple arrests on an unprecedented scale, particularly in relation to child exploitation and transmission of and accessing abusive images and videos.

As the books affirm, this is a developing area of the law – new laws, old laws adapted, and the need for ingenuity in law making in a field where technological advances mean that crime fighting may seem ever a step behind. One particularly interesting aspect is the cooperation between governments and corporations having a mutual interest in halting practices which can interfere with corporate and state security. The inclusion of 'warfare' in

Warren and Streeter's book is complemented by Kirwan and Power's coverage of terrorism.

For lawyers and law teachers seeking to engage with these new (and extension of old) practices, at a time when reliance on computer technology and the internet is ever-growing, ***Cyber Crime*** and ***Cyber Crime & Warfare*** will – along with more traditional casebooks – be a valuable addition to the library.