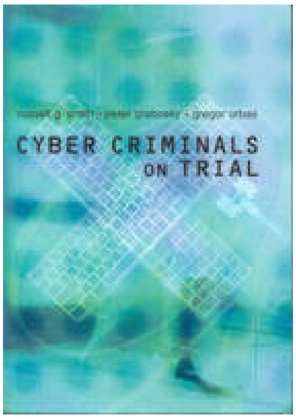
Book Review: Cyber Criminals on Trial

Cyber Criminals on Trial. Russell G. Smith, Peter Grabosky and Gregor Urbas. Cambridge University Press. August 2011.



What *were* the publishers thinking? For a fast-changing topic like cyber crime it simply will not do to re-issue in 2011, unaltered, a book from 2004.

The authors' original aims were fine: to examine the practical processes of investigation, prosecution and trial of cyber criminals. They set about their task by creating a database of prosecuted crimes, 240 of them, drawn from Australia, the UK and the US.

They begin their analysis with their own thoughts about defining "cyber crime". Almost everyone who writes about the topic has a preferred set of classifications but in reality there's no agreement. So many relatively ordinary crimes now have a cyber element simply because in many developed countries three-quarters of the population have personal computers and an even higher percentage mobile phones. For investigators the issue is how you handle digital evidence and what resources are required, not academic taxonomies.

Thereafter things pick up as the authors consider problems of perpetrator identification, decisions to prosecute, admissibility of evidence, problems of large volumes of evidence, and encrypted material. UK readers would probably have welcomed a more extended discussion of disclosure issues – in the UK it is a duty of the prosecution to disclose to the defence any "unused" material (collected in the course of investigation but not relied on as evidence) which may assist them.

There are useful studies of defences which apply to child sexual material: possession as a strict liability offence, proof of knowledge of possession, "legitimate research" as a defence and addiction. Other defences reviewed are contamination of evidence and "program errors".

The authors then ask whether cyber crime is punished differently from conventional offences and what the aims of punishment are – retribution, restitution, denunciation – and what forms they might take: confinement, forfeiture, restriction on computer / Internet access, community service and so on.

But there are many missed opportunities. Many of the UK cases were very familiar to me: in some of them I was instructed as a forensic expert, more often but not exclusively for the defence. For others I knew the details from the investigators, technicians and prosecutors involved. The authors had limited themselves to cases available via the usual legal reporting journals, occasionally supported by journalistic accounts. But cases are only formally "reported" if there is a legal issue. The one day meetings they had in London and the two days in Washington were not enough to identify important cases and their features.

The most startling omission is the UK National Crime Squad-instigated Operation Cathedral, mentioned briefly towards the end but not part of the database. This remains the largest ever multi-jurisdictional raid and occurred in 1998: 107 arrests in 12 countries of members of the paedophile Wonderland Club. The defendants eventually all pleaded guilty, there were no legal issues and so no formal case report. But had the authors taken more trouble they could have told their readers much about how the raid was organised, the evidence managed, the problems of handling encrypted material and disclosure to the defence.

Or take their case "28" which is the DataStream Cowboy/Kuji hack of 1994 and which came to UK trial in 1996 and 1997. This was an iconic teenage global hack with targets including USAF, NASA, various armaments companies and over 100 unclassified military computers. "Kuji", like Gary McKinnon many years later, had an obsession with Area 51 and alien spacecraft. The impact was sufficiently serious to prompt hearings in the US Senate; senators were originally told the attacks had probably come from North Korea and Latvia and were highly sophisticated. DataStream Cowboy was a 16-year-old London-based music student and Kuji was 19. In the end there was a quasi plea bargain for DataStream Cowboy and Kuji, partly because of mistakes in charging, walked free. But Smith and his co-authors don't tell the aspects that would have interested their readers: the immediate reason for the plea bargain was that police had not followed procedures in handling a 16-year-old. And there were also serious flaws in the prosecution evidence: digital material had not been properly preserved, was hearsay and the US authorities were refusing to disclose some of their technical methods. I thought these important enough to write an academic conference paper;

Google says it has now been cited 78 times so it is not that difficult to find.

But the 2004 cut-off date is the real problem. Towards the end of the book, the authors mention US Operation Buccaneer, an investigation into many interlocking “warez” groups, those who seek to acquire software, break any copy protection and then release it. The aim was hacker-notoriety rather than financial gain. The best-known group was “DrinkorDie”. The UK aspect was Operation Blossom and the final trial was in 2005. It cost £18.4m in legal aid alone and the reasons are worth examining. Instead of charging each suspect individually on the basis of the contents of their computers the Crown Prosecution Service charged conspiracy. The essence of that offence is the formation of a common purpose. As a result each defendant’s team had to examine all the other computers in the conspiracy – and those included individuals in the US and Australia. The evidence for the conspiracy was in masses of jargon-filled “chat logs”. There were issues about international disclosure and questions that the US authorities had used an agent provocateur – for which UK rules are much more restrictive. The CPS decision may have been within the framework of their internal Code but the heavy expense had almost no impact on eventual sentencing.

The decision not to update means that there is no mention of the big “phishing” cases where the “mules” and their organisers convert illegally acquired bank password details into real cash. Nor of the underground websites where batches of bank details, ATM skimmers hacking tools and botnets for hire are traded. One such was actually covertly run by a FBI agent. Readers today might also expect some discussion of Operation Ore, the exploitation of a database found at a US company that provided subscription fulfilment facilities for large numbers of websites selling access to paedophile material. In the UK there were 16,000 initial suspects, rapidly whittled down to 7,100, of whom some 2,400 were eventually convicted. Among the many issues was: as you can’t carry out 7,100 raids simultaneously, how do you avoid alerting suspects so that they don’t wipe their computers?

Perhaps for a book published in 2011 one can excuse no mention of Wikileaks, Anonymous and Lulzsek, particularly as these cases have yet to complete trial.

The authors’ analyses are useful but the missed opportunities are scandalous; almost as bad as thinking that a simple reprint was in any sense responsible publishing.

***Peter Sommer** is a Visiting Professor in the Department of Management at the LSE specialising in cyber security and digital evidence issues. His website is www.pmsommer.com*