Crime Law Soc Change (2017) 67:1–2
DOI 10.1007/s10611-016-9657-z

Overview

Michael Levi[1]

Published online: 1 October 2016

The articles in this volume deal with different dimensions of cyber-enabled crime and issues concerning the focus and the effectiveness of law enforcement responses. Most of the attention paid to the organisation of crime and to policing and its efficiency/effectiveness – terms often confused in practice – have understandably been conducted in the context of non-digital crime, or offline crime according to preference. Online crime presents major challenges of varied kinds: to prevention in our daily routines of activity, to traditional constructions of sovereignty, to law-making, to mutual legal assistance, to the attribution of offending, the recording of multiple crimes in multiple regions and countries, and to the pursuit and prosecution of offenders, whether connected to state-sponsored, state-tolerated or merely to 'ordinary decent criminals'. The papers in this volume contribute to various dimensions of this. In the first article, Levi examines trends in cyber-enabled financial crimes in a range of mostly advanced Western countries, and some evidence about their cost and harm. With some creative data analysis, for some operations (e.g., Décary-Hétu and Giommoni's study of Operation Onymous, Dupont's analysis of law enforcement in Canada – in this volume - and for some forms of payment card fraud in Europe) the activities against which policing efforts can be measured are reasonably knowable from public sources and sometimes even published. However for others, including the broader issues examined by Levi et al. in this volume, the error margins in the data (if there are any data at all) are often too great to know whether 'the problem(s)' is getting better or worse. The relationship between levels of crime and anxiety about crime is a further important dimension that has been studied more offline than online, and more for individuals than for businesspeople.

The measurement of direct and indirect intellectual property losses and even of fraud has been the subject of much dispute but in particular, the attribution of such losses to state-sponsored or state-tolerated attackers is often immensely difficult and hotly debated. This takes us beyond the tasks addressed in this volume, but it makes a

✉ Michael Levi
Levi@Cardiff.ac.uk

[1] Cardiff, Wales, UK

difference to our conception of harm and threat whether people are 'conscious opponents' and, by extension, what sort of conscious opponents they are. The articles that follow deal with what are sometimes characterised as 'ordinary decent criminals' operating in newer spheres, as well as more sophisticated and often younger 'teckies' alone or in collaboration with 'organised criminals', by which one might mean more than people who traditionally would have been professional robbers or drugs dealers, a dimension explored here by Leukfeldt, Kleemans and Stol in a novel and data-enriched manner.

Our aim in this volume has been to cast light on some important dimensions of online criminal organisation and on business, individual and policing responses to them, mostly in Canada and the EU, including the UK (for the present). However these have more global implications since the essence of cyber-enabled crimes and their reduction is that they present transnational challenges and it is almost impossible to use the nation state as a discrete unit of analysis.