Computer related crime features increasingly prominently in criminal statistics. As we move towards a cashless society where money is represented by data held on a computer system, so the range and scale of conduct is assuming almost epidemic proportions. Significant issues arise whether and where particular forms of conduct constitute criminal offences. These decisions have historically been a matter for national authorities. As with many issues covered in this book, the emergence of the Internet has brought about significant changes as it has become increasingly apparent that national legislation can be of limited effectiveness. Although cross-border conduct has occurred for very many years and the doctrine of extradition is a well-established one, such actions were the exception to a norm in which all aspects of conduct occurred in a single jurisdiction. The United Kingdom’s legislative history in the field of computer related crime date to the Computer Misuse Act of
9. National and international responses to computer-related crime

1990. In many respects, this legislation restated the position that had been reached under common law where a number of cases had determined that computer related conduct could be prosecuted under existing provisions of the criminal law. In 2001 the Council of Europe Cybercrime Convention was opened for signature and remains the most significant international instrument in the field, having been ratified by almost all European States and a number, including the United States, of non-European jurisdictions. As well as making provision for harmonising substantive criminal offences, there have been moves to enhance cooperation between law enforcement agencies at a procedural level.