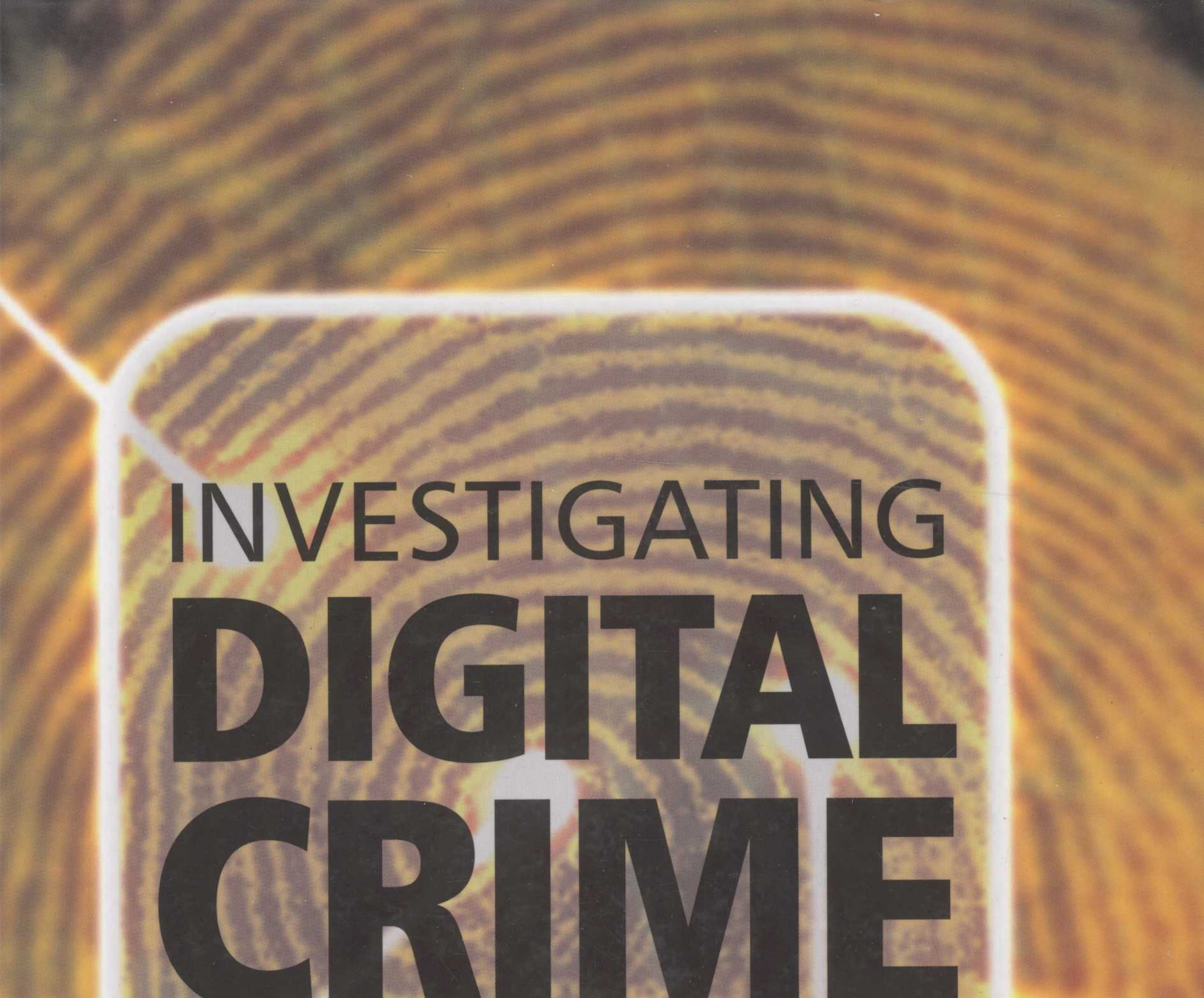
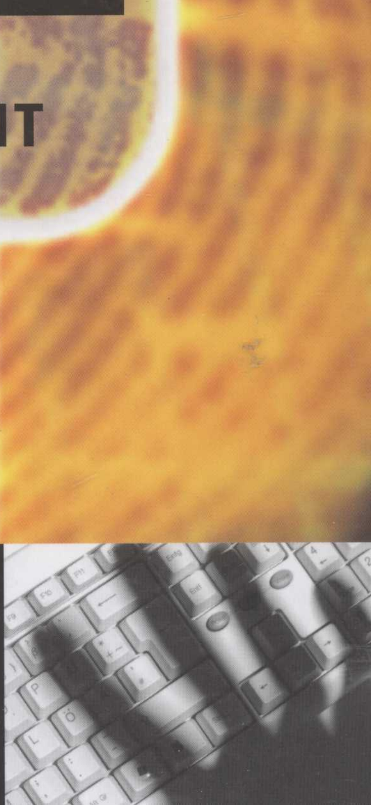


INVESTIGATING DIGITAL CRIME

EDITOR **ROBIN BRYANT**



WILEY

Investigating Digital Crime

Edited by

Robin Bryant

Canterbury Christ Church University, UK

John Wiley & Sons, Ltd

Copyright © 2008 John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester,
West Sussex PO19 8SQ, England

Telephone (+44) 1243 779777

Email (for orders and customer service enquiries): cs-books@wiley.co.uk
Visit our Home Page on www.wileyeurope.com or www.wiley.com

Designations used by companies to distinguish their products are often claimed as trademarks. All brand names and product names used in this book are trade names, service marks, trademarks or registered trademarks of their respective owners. The Publisher is not associated with any product or vendor mentioned in this book.

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold on the understanding that the Publisher is not engaged in rendering professional services. If professional advice or other expert assistance is required, the services of a competent professional should be sought.

Other Wiley Editorial Offices

John Wiley & Sons Inc., 111 River Street, Hoboken, NJ 07030, USA

Jossey-Bass, 989 Market Street, San Francisco, CA 94103-1741, USA

Wiley-VCH Verlag GmbH, Boschstr. 12, D-69469 Weinheim, Germany

John Wiley & Sons Australia Ltd, 33 Park Road, Milton, Queensland 4064, Australia

John Wiley & Sons (Asia) Pte Ltd, 2 Clementi Loop #02-01, Jin Xing Distripark, Singapore 129809

John Wiley & Sons Canada Ltd, 6045 Freemont Blvd, Mississauga, Ontario, L5R 4J3

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

Library of Congress Cataloging-in-Publication Data

Investigating digital crime / edited by Robin Bryant.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-470-51600-3 (cloth) – ISBN 978-0-470-51601-0 (pbk.)
1. Computer crimes–Investigation. 2. Commercial crimes–Investigation.
I. Bryant, Robin, Dr.
HV8079.C65I59 2008
363.25'968–dc22

2008012121

British Library Cataloguing in Publication Data

A catalogue record for this book is available from the British Library

ISBN 978-0-470-51600-3 (H/B)
ISBN 978-0-470-51601-0 (P/B)

Typeset in 10.5/13pt Times by Aptara Inc., New Delhi, India
Printed and bound in Great Britain by Antony Rowe Ltd., Chippenham, Wiltshire

Investigating Digital Crime

Preface

Robin Bryant

Extensive media coverage, numerous government and industry reports and frequent police warnings have all contributed to a heightened awareness of new criminal opportunities following in the wake of the rapid growth of digital technologies. If we are not quite yet living in Castells' (1996) 'network society' we are, in many key respects, close to it. Superficially at least, it might appear that we have entered a new era with new forms of criminality. However, on closer examination, many of these supposedly novel forms of crime (such as phishing in order to perform an identity fraud) in fact share much in common with conventional and long standing crimes and criminal techniques. Thus the reader will encounter an ongoing debate throughout this book concerning just how 'new' are they, in reality, these 'new technology' crimes? This debate culminates in a chapter concerned with some of the developing criminological and motivational perspectives on digital crime.

In the chapters that follow, we have deliberately chosen to extend the discussion beyond the realms of what may be termed 'conventional cybercrime' (despite the apparent inherent contradiction of the phrase) to other forms of criminality that exploit digital technologies to a lesser or greater extent. Hence we examine telecommunications fraud, video game piracy and 'chip and PIN' credit and debit cards, in addition to considering well-recognised problems such as cybercrime and internet grooming. It is for this reason that we have adopted the phrase 'digital crime' within the title of the book.

This book examines the legislative and investigative response to digital crime both in chapters exclusively devoted to this subject, but also more generally throughout the remaining chapters. Given the international nature of much digital crime the discussion of legislation also extends to the European Commission's Convention on Cybercrime.

Digital crime will undoubtedly continue to present the law enforcement community with new investigative challenges, particularly of a technical nature, and we have attempted to delineate these challenges alongside a description of current law enforcement practice. The professional backgrounds of the contributors to this book, drawn from the academic community (particularly computer science), police training and criminal investigation, reflect this desire to engage with the issues surrounding investigation.

A rapid pace of change creates an ever-present danger for the authors of a printed work exploring the impact of new technologies; the book could well be out of date by the time it is published. It is inevitable that when you read this text, at least some of the crimes we examine will have faded from public consciousness, and drifted down the priority lists of digital crime investigators. We have tried to head off this danger by attempting to draw conclusions of a more lasting nature, based upon observations of current (and perhaps more transient) forms of criminal activity, but illuminated by theoretical perspectives.

Each chapter concludes with a set of questions for the reader, either as a review of the material covered or as questions to stimulate further research into the topics.

Acknowledgements

The authors would like to thank Detective Constable Paul McLea from the Police Service of Northern Ireland for his invaluable advice on the legal issues surrounding encryption legislation in the UK; Ed Day for providing feedback on earlier drafts of a number of chapters, Sofia Graca for translation, Karen Preece and Gill Lennon for proofreading Chapter 3; Emily Wilkins for her help in the final proof-reading and finally, Katy and Emily Stephens for their patience, support and understanding whilst several of the chapters were being produced by Paul Stephens.

Reference

Castells, M. (1996) *The Information Age: Economy, Society and Culture. The rise of the Network Society.* **1**: Oxford: Blackwell Publishers.

List of Contributors

Robin Bryant is Head of Department of Crime and Policing Studies at Canterbury Christ Church University. He has edited and contributed to several books on police training and published and presented widely on investigative theory.

Sarah Bryant specialises in redrafting and editing academic material of a technical nature for a wider readership. Her academic background is in science education and the development of learning materials for adults. She has contributed to the editing of all of the chapters, and also created and developed a number of diagrams and other aids to understanding in this book.

Joe Carthy is a Senior Lecturer and Director of the Centre for Cybercrime Investigation at University College, Dublin. Joe has published widely on cybercrime investigation and computer security and is the author/co-author of 70 scientific papers and a textbook on computer architecture.

Denis Edgar-Nevill is Head of Department of Computing at Canterbury Christ Church University. He led the development of the MSc Cybercrime Forensics which is jointly validated and delivered with the NPIA.

Paul Gillen is a Detective Inspector within the Garda Bureau of Fraud Investigation, Dublin. Paul is also currently the Project Manager of the EU Agis programme 'Cybercrime investigation – delivering an intermediate level accredited modular international training programme'.

Tahar Kechadi is a Senior Lecturer at the School of Computer Science & Informatics at University College, Dublin. His research interests span the areas of parallel processing, parallel architectures, security of parallel computing, multi-stage interconnection networks, heterogeneous distributed systems, scheduling, dynamic load balancing, artificial neural networks, optimisation techniques and Grid computing.

Ian Kennedy is a forensic computer analyst within the Digital Forensics Unit of Kent Police, south-east England. In addition to his operational police commitments, he is also a regular guest speaker at digital forensics lectures and the author of numerous articles published both in print and on the internet.

Angus Marshall is a Senior Lecturer in Forensic Science at the University of Teesside where he is responsible for the digital evidence portfolio. He is also a practicing expert witness for prosecution and defence. He is notorious for crashing deadlines and the mere mention of his name makes editors quail. His real passion is motoring, quickly, in classic sports and GT cars.

Dave O'Reilly is a consultant in the area of computer networks and IT security, application development and project management. He has designed and supervised implementation of business IT systems for clients around the world. Dave teaches occasional courses on computer network technology. On several occasions he has advised the Garda Siochana as an expert on computer networking.

Paul Stephens is Programme Director for the BSc (Hons) Forensic Computing programme at Canterbury Christ Church University. He has worked with, and taught, representatives of law enforcement agencies from across the European Union on digital crime related issues.

Tracey Stevens is Deputy Head of Hi-Tech Crime Training at the National Policing Improvement Agency. For the past five years she has specialised in the development and delivery of training both nationally and internationally for those involved in investigating digital crime. She has contributed to a number of Best Practice Guides issued to law enforcement agencies in this specialised area of work, including guidance for managers of high tech crime units and for those searching for and seizing digital evidence.

All views expressed represent those of the contributors and not necessarily those of their employers.

All trademarks, product names, company names or logos cited herein are the property of their respective owners.

Contents

1 The Challenge of Digital Crime

Robin Bryant

In this chapter we examine the challenges arising from the growth of digital crime, particularly the problems faced by investigators. The interaction between technological change and criminality is well recognised for crime in general, but certain aspects of digital crime mark a significant shift both in the ways in which crime is enacted, and the consequent investigative response. This chapter explores some of the more general technological and social factors that have accompanied and possibly contributed to these changes. The remaining chapters consider particular aspects in more detail.

1.1 Technology and crime

Throughout history, general technological developments have continually created new opportunities for criminal activity, which in turn have driven the development of new technologies. Both the pre-modern and modern eras provide clear examples of such interactions. For example, in the 12th century, the techniques employed for counterfeiting currency closely matched the technological development of reliable methods to produce genuine currency. Similarly, bank robbers in the early 20th

Investigating Digital Crime Edited by Robin Bryant and Sarah Bryant

century soon began to use motor cars to speed their getaway, a scenario portrayed frequently in early Hollywood gangster movies such as *White Heat*. More recently, criminals employ advanced technology in their attempts to access internet-based banking systems in order to launder the proceeds of criminal enterprises.

The burgeoning development of a wide range of new technologies provides an ever expanding range of options for the creative mind. Some of the terminology relating to these technologies and their applications are shown in figure 1.1; no doubt digital crime investigators will already be familiar with the meanings of many of the terms shown.

Just as technology is utilised by many people for legitimate reasons, so it will be by those intent on committing crime. In this sense, little has changed; *plus ça change, plus c'est la même chose*. However, in the late modern age, crime that specifically exploits digital technologies (what we term in this book 'digital crime') has a number of possibly novel characteristics, and we explore these below.

1.1.1 Spatial and temporal differences

It perhaps now a cliché to observe that digital crime respects no international or legislative boundaries. However, it is undoubtedly true that much digital crime (particularly crime associated with the internet) is not anchored in time and space in quite the same sense as more conventional crime. Whereas the 1950s con artist inviting passers-by to 'Find the Lady' (pick out the Queen of Hearts from a row of three face-down playing cards) in London's Petticoat Lane would need to make direct personal contact to carry out the fraud, an eBay fraudster is not so constrained. Likewise, some crimes (such as installing a 'Trojan horse' virus) may be enacted in seconds, but the effect may not be felt until days, months or years later. Vatis (2005) goes so far as to claim that cybercrime in particular represents

> [. . .] the most fundamental challenge for law enforcement in the 21st century. By its very nature, the cyber environment is borderless, affords easy anonymity and methods of concealment and provides new tools to engage in criminal activity.

For digital crime, temporal differences are also significant, particularly in relation to the rapidity of interactions, such as receiving reward and gratification. The probable motivation for a person to illegally download the mp3 version of

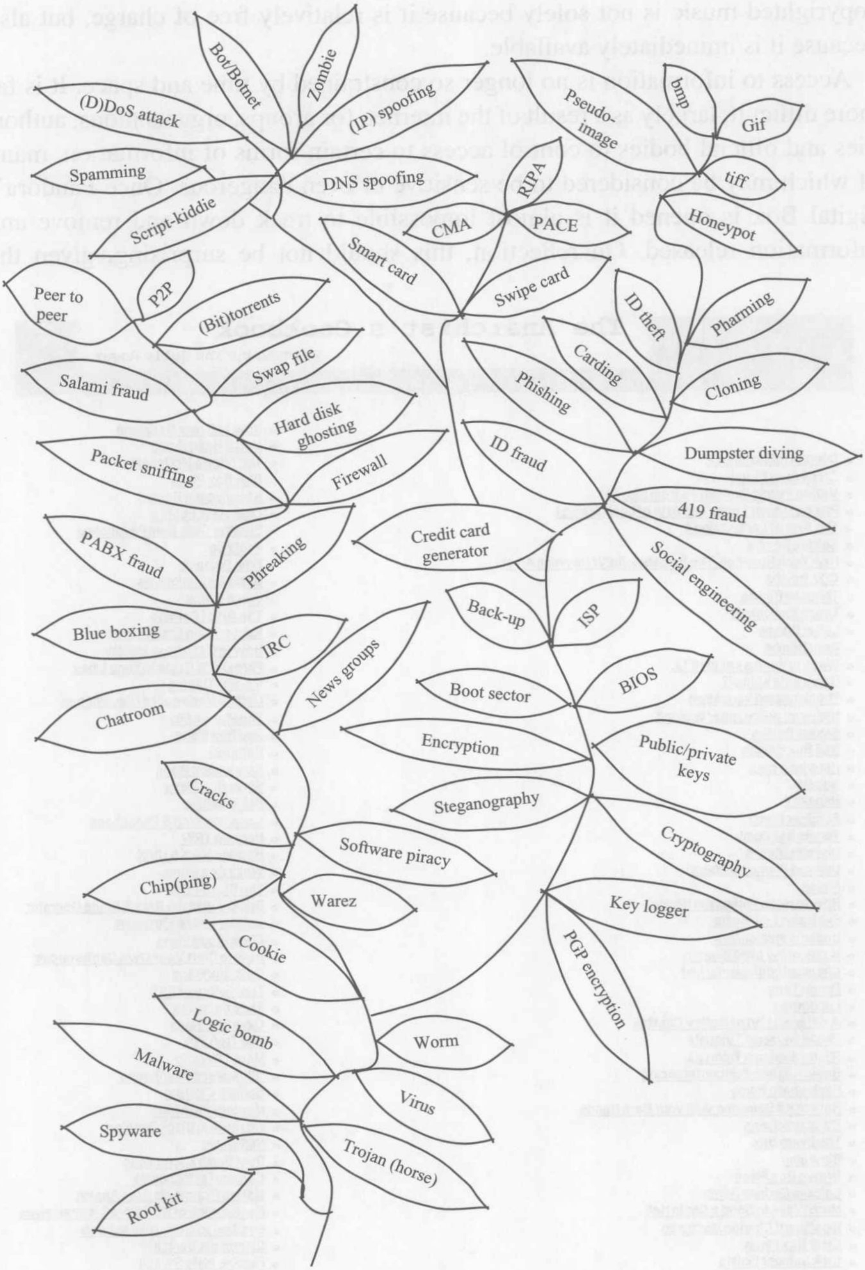
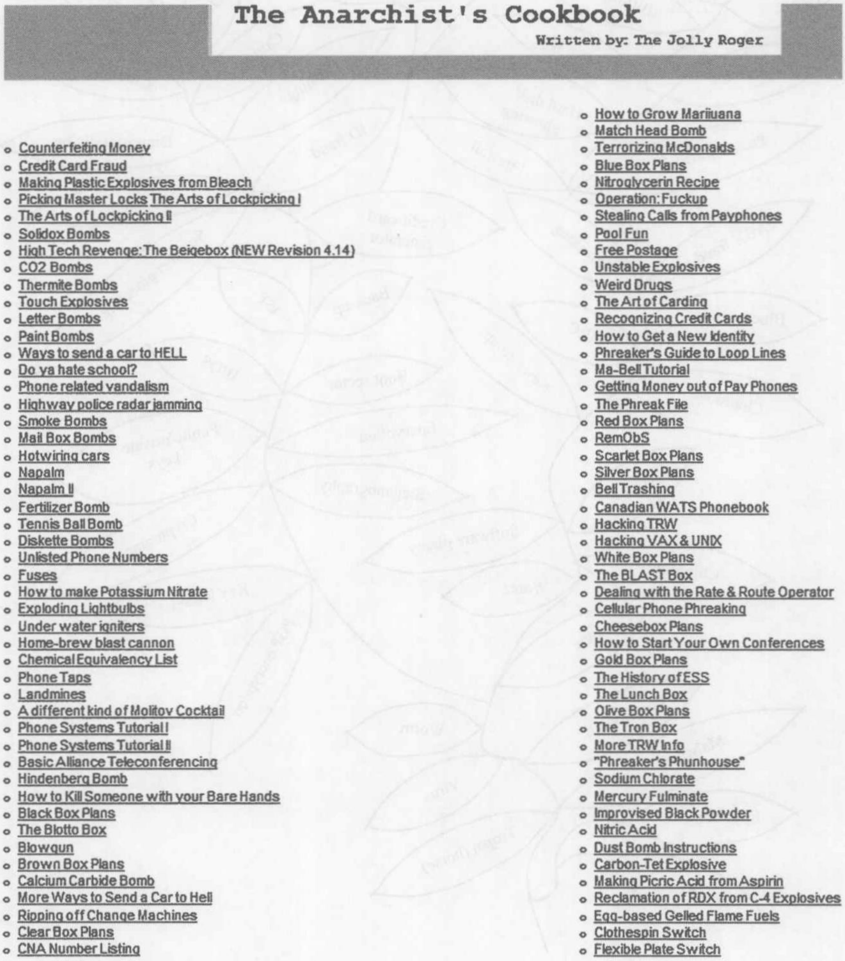


Figure 1.1 Digital terminologies (*Sarah Bryant*)

copyrighted music is not solely because it is relatively free of charge, but also because it is immediately available.

Access to information is no longer so constrained by time and space. It is far more difficult, largely as a result of the internet, for groups, organisations, authorities and official bodies to control access to certain forms of information, many of which may be considered to be sensitive or even dangerous. Once Pandora's digital Box is opened it is almost impossible to track down and remove any information released. On reflection, this should not be surprising, given the



The Anarchist's Cookbook

Written by: The Jolly Roger

- Counterfeiting Money
- Credit Card Fraud
- Making Plastic Explosives from Bleach
- Picking Master Locks The Arts of Lockpicking I
- The Arts of Lockpicking II
- Solidox Bombs
- High Tech Revenge: The Beigebox (NEW Revision 4.14)
- CO2 Bombs
- Thermite Bombs
- Touch Explosives
- Letter Bombs
- Paint Bombs
- Ways to send a car to HELL
- Do ya hate school?
- Phone related vandalism
- Highway police radar jamming
- Smoke Bombs
- Mail Box Bombs
- Hotwiring cars
- Napalm
- Napalm II
- Fertilizer Bomb
- Tennis Ball Bomb
- Diskette Bombs
- Unlisted Phone Numbers
- Fuses
- How to make Potassium Nitrate
- Exploding Lightbulbs
- Under water igniters
- Home-brew blast cannon
- Chemical Equivalency List
- Phone Taps
- Landmines
- A different kind of Molitov Cocktail
- Phone Systems Tutorial I
- Phone Systems Tutorial II
- Basic Alliance Teleconferencing
- Hindenberg Bomb
- How to Kill Someone with your Bare Hands
- Black Box Plans
- The Blotto Box
- Blowgun
- Brown Box Plans
- Calcium Carbide Bomb
- More Ways to Send a Car to Hell
- Ripping off Change Machines
- Clear Box Plans
- CNA Number Listing
- How to Grow Mariiuana
- Match Head Bomb
- Terrorizing McDonalds
- Blue Box Plans
- Nitroglycerin Recipe
- Operation: Fuckup
- Stealing Calls from Payphones
- Pool Fun
- Free Postage
- Unstable Explosives
- Weird Drugs
- The Art of Carding
- Recognizing Credit Cards
- How to Get a New Identity
- Phreaker's Guide to Loop Lines
- Ma-Bell Tutorial
- Getting Money out of Pay Phones
- The Phreak File
- Red Box Plans
- RemObS
- Scarlet Box Plans
- Silver Box Plans
- Bell Trashing
- Canadian WATS Phonebook
- Hacking TRW
- Hacking VAX & UNIX
- White Box Plans
- The BLAST Box
- Dealing with the Rate & Route Operator
- Cellular Phone Phreaking
- Cheesebox Plans
- How to Start Your Own Conferences
- Gold Box Plans
- The History of ESS
- The Lunch Box
- Olive Box Plans
- The Tron Box
- More TRW Info
- "Phreaker's Phunhouse"
- Sodium Chlorate
- Mercury Fulminate
- Improvised Black Powder
- Nitric Acid
- Dust Bomb Instructions
- Carbon-Tet Explosive
- Making Picric Acid from Aspirin
- Reclamation of RDX from C-4 Explosives
- Egg-based Gelled Flame Fuels
- Clothespin Switch
- Flexible Plate Switch

Figure 1.2 A typical hypertext version of the 'Anarchist's Cookbook'.

origins of the internet as a network designed to withstand attack. Contrast two documents produced in the 1970s: the so-called ‘Green Book’ produced by members of the Provisional IRA (to help train their recruits in the use of lethal weapons and quasi-military tactics) with the notorious ‘Anarchist’s Cookbook’, a text still circulating on the internet which details, inter alia, the manufacture of improvised explosive devices.

Most of the ‘military’ content of the Green Book was strictly controlled and ‘analogue’ in nature (presumably mainly photocopied and distributed on paper), and has not apparently been released into the public domain. However, the Anarchist’s Cookbook and similar documents (such as the Terrorist’s Handbook) have been developed and expanded by a number of contributors working independently and anonymously (now as part of a wider project termed the ‘Jolly Roger Cookbook’) and are readily available to anyone through the internet. In 1999 David Copeland (not believed to be a member of any terrorist organisation) used information contained in the Terrorist’s Handbook to construct nail bombs which he used to attack people in a gay bar in Soho in London, and then passers-by in Brick Lane and Brixton, both multi-cultural areas of London (BBC, 2000).

1.1.2 Economies of scale

Second, digital crime often exploits the ability of ICT to disseminate information widely, repeatedly and cheaply. As a result, what we might term the ‘sucker quotient’ for digital crime can be much lower than for conventional crime; for digital crime the investment of time and effort may be low, but the activity may still nonetheless provide high returns for the criminal. Our 1950s con artist is counting on quite a few people from those hundreds passing by to be gullible enough to take part in the con; the sucker quotient has to be relatively high for the con to yield sufficient results. On the other hand, a phisher can send tens of thousands of fake emails relatively easily, and even if only one victim responds, the resulting user account details may be used subsequently to commit identity theft and fraud, potentially very lucrative crimes. In a somewhat similar way, the pattern of rewards from other digital crimes follows the related principle of many victims and small losses. As Wall (2004, p. 20) suggests

> Where once a robber might have had to put together a team of individuals [. . .] in order to steal £1 million from a bank, new technologies are powerful enough (in principle at least) to enable one individual to rob one million people of £1 each.