

# Contents

<i>List of Tables</i>	viii
<i>List of Figures</i>	ix
<i>List of Abbreviations</i>	xi
<i>Acknowledgements</i>	xv
<i>List of Contributors</i>	xvi
1 Introduction <i>Martin Gill</i>	1
<b>Part I Security as a Discipline</b>	<b>19</b>
2 A History of Security <i>Robert D. McCrie</i>	21
3 The Study of National Security Versus the Study of Corporate Security: What Can They Learn From Each Other? <i>Craig Stapley, Suzette Grillot and Stephen Sloan</i>	45
4 Engineering Principles for Security Managers <i>Bradley B. Rogers</i>	66
5 Contributions of Environmental Studies to Security <i>Richard H. Schneider</i>	90
6 Forensic Security and the Law <i>Daniel B. Kennedy</i>	118
7 The Study of Intelligence and Its Contributions to Security <i>James D. Calder</i>	146
8 Criminology and Security <i>Graham Farrell and Ken Pease</i>	179
<b>Part II Crimes and Organizations</b>	<b>201</b>
9 Employee Theft and Staff Dishonesty <i>Richard C. Hollinger and Jason L. Davis</i>	203
10 The Extent, Nature and Responses to Workplace Violence Globally: Issues and Findings <i>Elena Licu and Bonnie S. Fisher</i>	229

11	Combating White-Collar and Organized Economic Crimes: Some Reflections on the Role of Security <i>Michael Levi</i>	261
12	Commercial Burglary <i>Rob I. Mawby</i>	281
13	Shoptheft <i>Read Hayes and Caroline Cardone</i>	302
14	Terrorism <i>Paul Wilkinson</i>	328
15	Information Security <i>Jason Crampton, Kenneth G. Paterson, Fred Piper and Matthew J.B. Robshaw</i>	358
<b>Part III Security Services</b>		<b>381</b>
16	The Security Officer <i>Alison Wakefield</i>	383
17	Store Detectives and Loss Prevention <i>Read Hayes</i>	408
18	Private Investigators <i>Tim Prenzler</i>	423
19	CCTV: Is it Effective? <i>Martin Gill</i>	438
20	Shrinkage and Radio Frequency Identification (RFID): Prospects, Problems and Practicalities <i>Adrian Beck</i>	462
<b>Part IV Security Management</b>		<b>483</b>
21	Management <i>Joshua Bamfield</i>	485
22	Risk Management <i>Mary Lynn Garcia</i>	509
23	Disaster and Crisis Management <i>Dominic Elliott</i>	532
<b>Part V Issues in Security</b>		<b>561</b>
24	Regulation of Private Security: Models for Analysis <i>Mark Button and Bruce George</i>	563

25 Corporate Security: A Cost or Contributor to the Bottom Line? <i>Dennis Challinger</i>	586
26 Trends in the Development of Security Technology <i>Clifton Smith</i>	610
27 Theorizing About Security <i>Giovanni Manunta and Roberto Manunta</i>	629
<i>Index</i>	658

# 1

## Introduction

*Martin Gill*

The nature of security threats is changing and so too are the types of responses. Worldwide there has generally been a move away from concern about nuclear bombs aimed at countries to terrorist attacks aimed at individuals, organizations and communities. The focus on a nation's ability to strike has largely been replaced by individual, community and organizational awareness to resist and react.

Yet in only some cases has security achieved a greater significance on the corporate agenda. In many ways security suffers from being a grudge purpose, important it may be, but it is not a welcome spend all too often associated with the unattractive features of a 'locks and bolts' approach, or what is its modern equivalent of 'cameras, tags and alarms'. Measures can be functional, but they are not always viewed as attractive and it is not always obvious to all parties what benefits they generate. Perhaps the real limitation of modern security management is that it has, in general, failed to talk the language of business not least in showing how it systematically impacts (positively or negatively) on the bottom line. There are of course many very effective security departments, some excellent security companies, and some extremely astute security personnel, but all too often security is seen as the poor relation both in the corporate hierarchy and as a member of the extended law enforcement family.

At least part of the reason for this is that the study of private/corporate security has to be regarded as an embryonic discipline, perhaps at the stage computer science was 30 years ago and environmental science 20 years ago. There are still major definitional problems that have never been satisfactorily resolved (see for e.g. Johnston, 2000; Johnston and Shearing, 2003). As many texts on security note, while in English 'security' and 'safety' are different words with different meanings, in other languages one word describes the two. And different disciplines use 'security' to refer to quite different things. For example, it can refer to security on the streets and in homes and then it becomes part of the discipline of policing or crime prevention, where it focuses on organizational assets it comes under the umbrella of security management and occasionally business or organizational studies. In a different way it can refer to the defence of a country where it becomes part of the discipline of war studies, or peace studies or defence

studies and so on. Indeed, the emergence of private military groups offers new forms of security and new areas of study.<sup>1</sup> Moreover, within these disciplines there is relatively little cross referencing (but see Chapter 3).

The problem of definition is not an abstract one deserving only the attention of academics, it has practical implications. On one level security regulators need to know what to include and what to exclude and definitions are crucial to guiding that choice. In a different way perceptions of what is a security context (see the final chapter of this book for a discussion) will influence what is an appropriate security response. As Johnston and Shearing (2003: 3) note:

Our objective 'sense of security' (our feelings of safety) is just as important to most of us as any objective measure of our 'actual security' (i.e. the risks that we actually face). However, if the discrepancy between the two grows too wide, we are liable to be warned either that we have a 'false sense of security' or that we are 'paranoid'. Thus, to be effective security measures must address our subjective perceptions as well as more objectively identifiable threats to our safety.

The fact that security is still evolving as a distinct area of study in part explains the reason for preparing this book. Later the content and the rationale will be introduced but as a backdrop there are two issues that are in different ways core to assessing the current state of security. The first involves a short commentary on the extent of security which includes a consideration of the way it is provided, and second, a review of what we know about good security in terms of its effectiveness.

### **Security: here, there and everywhere**

Security is omni-present; there are clearly limits to what the State can provide (see, Garland, 1996)<sup>2</sup> and this has enabled the private sector to flourish.<sup>3</sup> Private security has expanded (see George and Button, 2000),<sup>4</sup> and in many ways the services offered mirrors and then extends those of the State. As Johnston and Shearing (2003: 32–3) drawing on the work of a range of studies note:

It is now virtually impossible to identify any function within the governance of security in democratic states that is not, somewhere and under some circumstances, performed by non-state authorities as well as by state ones. As a result, policy-makers are now ready to accept that the effective governance of security requires co-operation, collaboration and 'networking' between partners and that exact demarcation between the respective responsibilities of partners may be difficult, or even impossible to establish.

In practice partnerships can be problematic (although what partnerships aren't at least from time to time?), not least because the parties involved emerge from a set of conflicting principles (see, Prenzler and Sarre, 2002). In general, the private

sector is accountable only to those who pay for it, and it is geared towards profit, somewhat in contrast to providers of state services. Each type of service generates different benefits and associated with some limitations leading Johnston and Shearing (2003) to advocate a 'nodal' approach with the nodes representing a set of 'shifting alliances' consisting of state sector, corporate or business sector, non governmental organizations, and the informal or voluntary sector. As they point out (p. 148):

... by linking up – or 'networking' – non state nodes of security with each other, and with state nodes, it is possible that some of the strengths of 'private' forms of provision may be maximised, and some of their dangers minimised.

There are a range of reasons why partnerships are problematic. Indeed, the study of the privatization of security has included fairly extensive discussion in the literature where a prime focus has been the relationship between private policing and alternatives forms of provision (especially the State) (e.g. Bayley and Shearing, 2001; Button, 2002, 2004; De Waard, 1999; Gill and Hart, 1997; Johnston, 2000; King, and Prenzler, 2003; Prenzler, 2004; Prenzler and Sarre, 2002; Sarre, 2005; Sarre and Prenzler, 1999, 2000; Shearing, 1992). The difficulties in a partnership approach extend beyond mere ideological differences (see, McLeod, 2002; Rigakos, 2002). For example, the method used by Governments to allocate budgets is generally prescriptive specifying how money should be spent. It would seem much more sensible to provide a budget to the local police chief and ask him or her to develop a policing plan responding to local circumstances that would then need to be approved by local representatives. It may be prudent to have fewer police and more support officers, or perhaps some of the money spent on police would be better spent providing administrative help or specialist private security expertise. Indeed, the way budgets are allocated has as much to do with the limited role of security as any ideological differences, and as security develops an expertise in a march to professionalization it could be the main factor that keeps it at arms length.<sup>5</sup> Certainly, it should not be assumed that the public are against the use of private security officers in public space (Noakes, 2000).

Already it can be seen that the term 'private security' used as an umbrella phrase can refer to different activities. Table 1.1 is an attempt to highlight some of the ways in which security can be provided in what I have called 'The Mixed Economy of Security'. For each type or sector of provision some of the key ways that security is provided are listed with examples. Thus although it is not uncommon to discuss policing provision in terms of private, public, voluntary and informal (see Gill and Mawby, 1990a, b; Mawby, 2005) breaking these down further illustrates the very varied types of ways in which security can and is supplied and paid for. Private does not just mean a security company providing its services directly to clients, there might also be an internal market within an organization, even a public one. Or individuals working for an employer may spend some of their time working for someone else, including for the benefit of the

Table 1.1 'The mixed economy of security'

Type of provision	How security service is provided	Service provided to whom	Who pays	Example	Range of services
Private	Directly by company	To whoever will pay	The client	Personnel typically works for a security company and the company is contracted by a client to offer some types of service.	Potentially any type
	In-house/ Proprietary	To the employer	The company/ organization pays for its security personnel as employees alongside other staff	In-house officers are different from State officers because the employers are not state organizations, as such powers will most likely be restricted. Security officers work directly for the company/organization and are not normally clients.	Potentially any type
	In-house/ Proprietary	To parts of the employer organization who will pay	Other parts of the company or Group of companies	Until a few years ago, the Security and Investigation Service sold their services to 21 business units within the British Royal Mail Group. Effectively services are provided under contract.	Potentially any type
	By employees	An organization or company chosen by the employer.*	The employer	Some train companies agreed to pay for staff to be employed by the British Transport Police. The train companies pay and the police deploy. This has required a cultural shift on the part of both companies.	Usually restricted
	By employees	To the public	The employer	Some retailers in London have agreed that their staff can serve as Special Constables (police volunteers) while on duty. In this role they are providing a service to the community.	Mostly routine tasks

**Table 1.1** 'The mixed economy of security' – *continued*

Type of provision	How security service is provided	Service provided to whom	Who pays	Example	Range of services
State	Directly by the State	To the public	The State	<p>In the UK the police may formally accredit some individuals to help support policing. They have limited powers and sometimes none at all, but are invested with a duty to assist the police. Some private security officers have been accredited and they may undertake this work during working hours.</p> <p>The State employs a wide range of security personnel, including private security personnel to protect public buildings. Of course, a range of law enforcement and military personnel are employed directly by the State.</p>	Potentially any type
	Directly by the State – (mostly) external market	To whoever will pay who fall within ambit (usually regulated)	The State	<p>'Police Security Services Branch (PSSB), which is a publicly-funded body employing public servants who are not sworn police officers, competing in the same market-place with private security firms in providing fee-for-service security advice, protective security risk reviews, alarm monitoring, patrol and personnel services.'</p> <p>(Sarre, 2005: 60)</p>	Usually restricted by Statute

Table 1.1 'The mixed economy of security' – *continued*

Type of provision	How security service is provided	Service provided to whom	Who pays	Example	Range of services
	Directly by the State – (mostly) internal market	To other State (like) organizations prepared to pay for the service	State (like) organizations	'The Australian Protective Service (APS), which acts under the auspices of the Commonwealth Attorney-General's Department. Established in 1984, the APS is a government agency that provides a specialist protective security to government departments on a contractual "fee-for-service" basis.' (Sarre, 2005: 60)	Usually restricted by Statute
Voluntary/ Charitable	By individuals	To the community usually locally	Effectively provided free, may sometimes include bursary	Lots of 'security-related' agencies use volunteers to enhance the work they do. The police, prison service and probation service all use volunteers.	Usually restricted
	By individuals (sometimes as part of a group) By groups (sometimes individually)	To the immediate community By vigilantes to those defined as in need	Effectively provided free of charge By voluntary contributions	'Watch' schemes, the most commonly referred to is Neighbourhood Watch Guardian Angels	Usually restricted to routine duties Restricted
Informal	By individuals	To family members	No payment as such, mostly a social and sometimes legal obligation to look after each other	Parents are obliged to look after their children to protect them from harm, and most importantly, to educate them on how to protect themselves from danger.	All encom-passing

**Table 1.1** 'The mixed economy of security' – *continued*

Type of provision	How security service is provided	Service provided to whom	Who pays	Example	Range of services
	By individuals	To neighbours and friends	By individuals to neighbours and friends although the costs are usually in time spent	Security is often provided informally. Keeping an informal watch over neighbours' property while they are away is one example. Promoting security amongst family and friends is another example. Some positions have an informal role in promoting security, caretakers and janitors being examples.	Usually restricted

\* All employees and not just those in a security function, may play a part in providing security within the company and beyond, by, for example, looking out for trespassers and 'strangers' on the premises, or by looking for and reporting suspicious behaviour on the way to and from work and while out and about. Sales assistants may have a role in assisting with fraud prevention. In some countries, the USA being a case in point, police officers may work in private security when off duty.

public. Public employees may become involved in different ways too, and the voluntary sector can include anything from benign vigilantes<sup>6</sup> to police volunteers. And the informal sector is a major provider of security, considerable protection is provided by the family and friends and neighbours.

The main purpose here is to illustrate the varied and very different ways in which security is provided and to note that there are different implications in terms of quality and type of service, and accountability issues in these diverse arrangements, and this is likely to have different implications for measures of effectiveness too. This is not intended to imply that there is a best way of providing security, they all might be best for particular circumstances, it is more a case of truly understanding the dimensions of each in order to understand what is appropriate or best in a given context. Clearly, the next important step (other than to refine and improve Table 1.1) is to assess which types of provision are suited to a particular set of circumstances and to try and highlight the strengths and weaknesses of each and to compare them. It says much about the state of research on security and private policing that these issues have yet to be put under the microscope. Doing so will entail a broader multi-disciplinary approach, and will certainly require researchers to move outside the boundaries of single disciplines (Johnston and Shearing, 2003).

### **How good is security?**

There is a common-sense answer that it must be good. Few people, it seems, doubt the wisdom and certainly appear to accept detailed screening at airports, or the need for access controls to some premises. And evidence that security is valued can be derived from business practice which continues to purchase security, and in some cases invest more each year (Collins *et al.*, 2005). It is difficult to imagine bottom line focused organizations continuing with investments that they thought they could do without or did not believe were working. But of course this does not mean to say that they have carefully costed this, nor that what they have is the best. Indeed, many organizations do not have developed return on investment models for security operations, and few companies, and this includes security manufacturers and suppliers have collated credible independent evidence that their products specifically work to achieve clients' objectives. Too often a range of measures cause an effect and it is not always easy to identify which ones can claim credit for the success.

This does not mean to say that there is no good evidence of security working both effectively and cost-effectively (see Welsh and Farrington, 1999). But the problem is that there is relatively little research explaining what works and why, or for that matter what does not work and why which is arguably just as helpful. Within the criminology literature there has been a lot of work devoted to reducing opportunities for crime by applying a range of 'situational prevention' techniques. In a recent review of the approach (Clarke, 2005), its main proponent, Ron Clarke, has helpfully outlined a defence against some of the main criticisms of situational prevention although, from my point of view at least, it misses one

important element, and that is that situational prevention over simplifies the solution. As an approach – and it provides an excellent framework for security – it has not so far located itself within a management framework, yet many security projects/measures fail to succeed because they are poorly conceived or because they are badly implemented (for example, see, Gill and Spriggs, 2005). It is all too easy to claim that a measure or measures have not worked without being clear why, was it a failure of the measure, or the way it was implemented, in short a failure of theory or practice?

Corporate security is a world desperate for more quality evaluations helping to explain what works, what does not and crucially, why this is the case. Certainly there is a greater need for evaluation approaches that are more practical for end users. And most importantly, there is a need to communicate the findings to those at the sharp end of practice. Indeed, the whole process of communicating findings effectively to audiences who have learned to be sceptical of ‘academic’ studies is a task in itself. Very little attention has been paid to identifying specific skill sets and thinking through how these can be communicated or translated into training programmes aimed at practitioners and policy makers. Indeed, much more information is needed on how practitioners absorb information and the forms they need it in in order to make the most use of it. Certainly the timescales of research and evaluation do not meet the more immediate requirements of those charged with taking actions that require more immediate solutions. And there has been a lack of investment in security theory looking at developing principles and testing theory application in different contexts.

There is one other thing that needs to be discussed in the context of the study of private or corporate security, and that is a body of writings which question its value or perhaps more its role in democratic societies. This is not necessarily a Marxist critique that calls for the overthrow of anything private, more a case of a critical approach to the role of (private) security that is potentially divisive in a democracy because it is accountable only to those who can pay. Loader (1997a) is concerned about the inequalities of private security provision, in that it is provided on the basis of an ability to pay and ‘without reference to the common good’. It can be especially problematic, ‘if those able to secure protection in the market place begin to resent paying – through general taxation – for public policing (on the grounds that they will then be paying twice)’ (p. 385). Loader’s point is not that all security should be provided by the State, more that there are issues about how private security is provided that should concern all democratic societies, or, specifically:

What kinds of limits would a political community committed to equal citizenship and concerned to encourage social cohesion among its members place on the market exchange of security provision? (p. 385)

In a similar way Zedner (2003: 179) notes in the conclusion to her paper entitled ‘Too Much Security?’; ‘I have sought to show that the pursuit of security is by no

means an unequivocal good,' and she does this by identifying six paradoxes of security, these are:

... that security pursues risk reduction but presumes the persistence of crime; that the expansion of security has enlarged not diminished the penal state; that security promises reassurance but in fact increases anxiety; that security is posited as a universal good but presumes social exclusion; that security promises freedom but erodes civil liberties; and finally that security is posited as a public good but its pursuit is inimical to the good society. (pp. 179–80)

There is not the space here to examine these arguments (see also Loader, 1997b), and others like them, but they do offer an important counter to the belief that security can only be a good thing (see also, Brodeur and Shearing, 2005), understandably perhaps a view held by those who work within it. These writings principally question the social role of security, but economically it has long been recognized that organizations, and especially those in business need to build an economic as well as social rationality into protecting themselves. Retailers could do a lot more to prevent shop theft, they could put more goods behind counters, employ more staff, search all customers entering and exiting the store and so on, but this is not economically rational.

These critiques are fundamental to developing a rigorous body of knowledge for the study of security. It is this last point that brings us back to the purpose of this book containing, as it does, a range of insights and critiques into the study of security. The next section introduces the main areas of focus and outlines a little more about the content of each chapter.

## **This book**

At a security symposium held in the USA delegates discussed the various subject areas or disciplines that contribute to security, and, after some debate concluded that there were none that didn't. Moving on to consider areas of trade or activity where security was important, the delegates concluded there were none where it was not. Security then, to a lesser or greater degree, is a facet of every feature of our lives. The difficulty of prioritizing the areas of interest and focus will no doubt have troubled writers and editors of many a security text, and it certainly has this editor of this book. Therefore, the process by which topics and authors have been chosen is perhaps worthy of comment.

In each section of the book it will be easy to think of other relevant chapters that could, or even should have been included. In my judgment the chapters for this Handbook provide the foundation on which future editions may build. The authors were chosen because they are scholars with a recognized expertise in their area. It may be of some interest that of all the authors that were approached and asked to contribute only one was unable, because of illness. Precisely because they are all experts, they were invited to propose their own outline for the chapter taking into account the need to provide an authorita-

tive review of research, current issues and thinking in their area of expertise. Their initial outlines were sometimes modified, often to avoid overlap,<sup>7</sup> but never to any great extent. Once the chapter outline was agreed authors were typically given about 12 months to think about and write their contribution. When it was received it was sent for independent review, and suggestions and ideas were sent back to authors who were asked to prepare a final draft taking account of any recommendations that had been made.

### **The content**

The first section of this book considers security as a discipline. In Chapter 2 Bob McCrie traces the history of security showing how it facilitated the development of early civilization and has remained a core part of the functioning and development of individuals, enterprises, institutions, regions, and nations. His account marks the impact of industrialism and modernism on the creation of the modern military, public policing, and the private security industry.

In Chapter 3 Craig Stapley, Suzette Grillot, and Steve Sloan argue that the fields of corporate and traditional security studies have not readily adjusted to the changes in international affairs. They argue the need to bridge the gap between traditional and corporate security studies, not least because the modern world where the distinction between domestic and foreign threats has become blurred, and where 'non-state' actors are increasingly challenging the monopoly of force and the centrality of the State on the international stage.

In Chapter 4 Brad Rogers examines the contribution of engineering studies to security. He notes that most managers responsible for the engineering of solutions to security problems are not professional engineers, but may benefit from a greater understanding of the engineering design process. He examines a security system as a collection of interacting components, policies and procedures that are integrated and organized to react to a malevolent human attack in a manner that results in a protected asset and a defeated adversary. He outlines a methodology that is appropriate for examining all security systems.

In Chapter 5 Richard Schneider examines the link between environmental science and security. Schneider shows that while research and practice suggest there are broad place-based crime prevention theories that describe and predict criminal behaviour, the application of effective security design tends to be context dependent. For him environmental studies related to security demonstrate the importance of theory and practice influencing each other and spurring new developments in each.

Chapter 6 tackles the study of forensic security and the law. Daniel Kennedy shows how responsibility for security shortcomings which result in attack, can be attributed. He discusses 'crime foreseeability' and shows how it can be established by examining a property's criminal history and social ecology and how this can then be linked to determining what is or should have been an appropriate security response.

In Chapter 7 James D. Calder suggests that the lack of a scholarly approach in security studies could be corrected by learning from the study of national

security intelligence, particularly in terms of the research and analysis functions that became core elements in most post-World War II national security decision processes. Similarly in Chapter 8 Graham Farrell and Ken Pease highlight the historical lack of interest by criminologists in security, albeit that the 'situational crime prevention' framework is a good one for studying security. The main contribution of criminology to the security industry is, the authors contend, to provide a range of approaches and tools for preventing crime and thereby an understanding of the mechanisms whereby they are likely to succeed or fail. They note the development of a discipline of Crime Science by the incorporation of contributions from a range of crime-relevant science disciplines.

The second section of this book assesses studies of offence types that are associated with organizations. Once again this does not cover all offences although in the space available the focus has been on those that are prominent. In Chapter 9 Richard Hollinger and Jason Davis discuss the study of dishonest staff. They note that employee theft is the single most costly form of larceny experienced by the business world, and that in some work settings, from a statistical standpoint, the 'deviant' employee is the worker who is *not* stealing. No wonder then that a major proportion of business failures are directly or indirectly related to employee theft or dishonesty. They trace various ways of explaining dishonest behaviour which is a basis for determining effective responses. Intriguingly they note that some companies tolerate some offending because it is significantly less expensive than paying employees a more equitable wage. They suggest a combination of strategies to guide the study and practice of security.

In Chapter 10 Elena Licu and Bonnie Fisher examine issues relating to workplace violence. They helpfully take a global perspective examining definitional issues, the scale of victimization and characteristics that are most likely to result in it, as well as documenting the negative physical, psychological and financial toll on employees and the organization. The authors suggest a focus for prevention efforts that is derived from evidence-based research.

In Chapter 11 Mike Levi tackles the issue of white collar crime. He looks at the features that render organizations more vulnerable to both fraud and money laundering and the connections between them. He moves on to assess responses and examines the management of reputational damage, the actual and appropriate roles of the criminal law and policing in the mitigation of business fraud and money laundering risks, and the role of collective business action against white-collar crimes.

In Chapter 12 Rob Mawby discusses research on commercial burglary across the world. He finds that while the extent of commercial burglary varies between countries, it is universally more common than household burglary. And the impact is considerable in financial and emotional terms. Despite this he finds that business people are sometimes ambivalent about the threat posed by burglars, and demonstrate a reluctance to invest in security. Conversely retailers have invested heavily in security to prevent shop theft, the focus of Chapter 13. Read Hayes and Caroline Cardone found the impact to be considerable, in addi-

tion to the obvious financial loss offences also disrupt processes, reduce product availability and introduce violence into shops. Their analysis of various patterns of offending leads them to assess the characteristics of an effective response.

In Chapter 14 Paul Wilkinson seeks to clarify our understanding of the concept of terrorism and other forms of violence, and the New Terrorism of the al-Qaeda Network and its implications for security are examined highlighting its capability for mass-casualty attack in western cities as well as its continuing intensive terrorist activity in the front line states in the Middle East. Wilkinson observes that terrorists have only rarely attained their strategic objectives by terrorism alone, although the events of 9/11 underline the enormous impact they can have. An outline is provided of the main elements of an effective strategy to dismantle the al-Qaeda Network including the management of the media.

In Chapter 15 Jason Crampton, Kenneth Paterson, Fred Piper and Matthew Robshaw discuss the latest developments in information security research. Their discussion focuses initially on cryptographic algorithms. They argue that while they often enjoy a highly visible public profile, in practice they are only a very small part of the security solution. They note that the security features offered by modern computer systems are improving all the time, but care must be taken when configuring these features to ensure that they implement the security required. They argue the case for an effective programme of information security management.

The third section of the book includes five chapters on key security services and products, three of these focus on people services and two on technology, although they overlap. In Chapter 16 Alison Wakefield assesses the role of security officers, which as she notes, are omnipresent. She argues that the development of the security industry has included the emergence of new and increasingly sophisticated opportunities for security personnel. Consequently the stereotypes of unskilled, uneducated security personnel may have become less relevant as the industry has moved into more demanding and prominent areas of work. Thus, in jurisdictions such as the UK and many US states, low pay and long hours belie the growing levels of responsibility for security officers, while reward levels in some European countries suggest that lessons may be learned through international comparisons. Her analysis includes a discussion of the role of private security in and with law enforcement. In Chapter 17 Read Hayes tackles another type of security delivered by people, the under-researched area of store detectives. He discusses their role and assesses the impact they have in stores concluding they have a vital role to play in the protection of assets.

In Chapter 18 Tim Prenzler assesses the role of private investigators which he sees as extremely diverse and often highly sophisticated, including covert surveillance, legal enquiries, fraud investigations, debt recovery, serving of legal notices, tracing missing persons, forensic accounting and security risk assessments. He assesses the potential inequalities and injustices that can result from the expansion of forms of 'private justice' based on a clients' capacity to pay. He welcomes licensing to protect clients and innocent third parties from poor quality service and from violations of civil liberties.

In Chapter 19 I discuss research on CCTV and in particular assess the evidence on its effectiveness taking a broader approach than just a consideration of the impact on crime rates. Although this is important, the extent of CCTV and the concerns about intrusions into people's civil liberties also matter. Discussion is also focused on the impact of CCTV on the public's feelings of safety and the pressing worry that CCTV merely displaces crime. In short, it is argued that while CCTV may well become, if it has not already, the essential security tool there is still a lot of learning to be done to use it to maximum advantage.

In Chapter 20 Adrian Beck evaluates research on RFID which, as he notes, is viewed by some as the next generation of barcode, enabling products, cases and pallets to be identified uniquely and without the need for direct human intervention. Beck believes it could revolutionize the way in which supply chains are managed and protected but is less convinced at its potential to seriously impact on theft by staff and customers. In any event he argues that there are still many technological hurdles standing in the way of the wider adoption of RFID and consumer concerns about privacy have yet to be fully addressed. For Beck RFID should not be seen as a panacea to the problems of shrinkage, as it clearly is not, but more as a potentially powerful tool to enable stock loss practitioners to manage the problem much more effectively.

The fourth section of the book focuses on management issues. In Chapter 21 Joshua Bamfield assesses the role of security as a part of management, dealing with planning, leading, organization, controlling, staffing, co-ordinating, and motivating. He examines the role of the security manager including their responsibility for configuring key variables including *tasks, structure, information and decision processes, security investment, reward systems, and people* to produce the greatest security results from a given security budget without imperilling the organization's future.

In Chapter 22 Mary Lynn Garcia discusses security risk management and specifically its focus on risk assessment, which attempts to establish what can go wrong, the likelihood that this will occur, and the consequences. The answers to these questions help identify and evaluate risks. She contends that risk management builds on risk assessment by considering available options, their associated tradeoffs in terms of costs, benefits, and risks, and the impacts of management decisions on future options. Her analysis incorporates a discussion of the business case for security and the options for a response including the use of avoidance, reduction, spreading, transfer, and acceptance alternatives.

In Chapter 23 Dominic Elliott discusses how some organizations possess crisis prone characteristics and how an organizational crisis can result from the actions and inactions of management regardless of the events that trigger them. He notes how crises possess both technical and human characteristics which both need to be effectively managed. Importantly, he discussed how managers may learn from the study of organizational failures elsewhere and how the process of Business Continuity Management provides an opportunity to identify potential weaknesses, the resources and competences required to meet customer needs and to develop crisis resilience alongside contingency plans.

The fifth and final section of the book is focused on a range of issues central to any discussion of modern security management. In Chapter 24 Mark Button and Bruce George discuss models of regulation including radical ones, and they draw upon world-wide experiences. They also refine and develop the model of private security regulation they initially presented in 1997. In Chapter 25 Dennis Challenger assesses the impact of security on the 'bottom line'. He argues that corporate security delivers value to a corporation through a range of activities the absence of which would likely lead to losses. For Challenger there is potential for a properly embedded security programme to contribute its expertise to all parts of the business.

In Chapter 26 Clifton Smith reviews trends in security technology. He argues that the application of security technology to protect assets needs – amongst other things – to be justified according to established criteria such as theories and principles, and uses the *defence in depth* and *crime prevention through environmental design* frameworks to guide his analysis. A hierarchy classification of intrusion detection systems is presented in an attempt to classify different types of security technology systems. He ends his analysis looking at the potential of security technology in the future.

In the final chapter Giovanni and Roberto Manunta theorize about what is a security context or situation and therefore what is not. They outline a methodology which invites readers to look at security as part of a much wider set of processes. They argue that to be effective a security system must be driven by a set of ethical, political and economic considerations proper to its specific context, level of analysis and situation. To be effective and useful as a system, security needs a clear definition of scope, relations and goals, of inputs, processes and outputs and they suggest how this might be achieved.

And so this is the first edition of the Handbook of Security. What it confirms, as if it needed confirming, is that security is a broad subject as a practice and as a discipline. It would be possible to envisage a book this size on each of the chapters presented. But it is a foundation on which to build. Indeed, I would be delighted to receive your thoughts on the content of this Handbook, and your suggestions on topics you believe should be covered next time around.<sup>8</sup> The development of the security body of knowledge is inevitably a long intellectual journey, this book can perhaps best be viewed as a small contribution along the way.

## Notes

- 1 See interview with Clifford Shearing in the International Observer, produced by the International centre for the Prevention of Crime; [http://www.crime-prevention-intl.org/io\\_view.php?io\\_id=125&io\\_page\\_id=559](http://www.crime-prevention-intl.org/io_view.php?io_id=125&io_page_id=559)
- 2 Much police work is not crime-related (see, Bayley, 1996), indeed only a small proportion of the police strength is on the beat at any one time (Morgan and Newburn, 1997).
- 3 For a good discussion of the expansion of private security see, Jones and Newburn (1998).
- 4 It is worth noting the growing recognition that all staff in a company fulfil a security function. In a recent study of shop theft conducted by the author, shoplifters drew

attention to sales staff interest in them being a deterrent, good customer service is an effective crime prevention measure.

- 5 It needs to be emphasized that whatever plan emerged would need to be agreed with local representatives but it would mean that the full range of different forms of security provision could be incorporated into a single plan.
- 6 A malign form would be organized protection rackets which can inflict serious violence. They are of course another way of providing security illustrating still further the dimensions of the 'mixed economy of security'.
- 7 There has been no attempt to present a specific line of argument in this book, indeed that would be counter productive. Rather the objective has been to tap into the expertise of the authors in defining the salient themes and issues. Unsurprisingly then, as will become evident, contrary views emerge.
- 8 Please forward any suggestions or ideas to Martin Gill on, m.gill@perpetuitygroup.com.

## References

- Bayley, D.H. (1996) 'What Do the Police Do?'. In Saulsbury, W., Mott, J. and Newburn, T. (eds) *Themes in Contemporary Policing*. London: Independent Committee of Inquiry into the Roles and Responsibilities of the Police.
- Bayley, D. and Shearing, C. (2001) *The New Structure of Policing: Description, Conceptualization and Research Agenda*, Research Report NCJ 187083. Washington DC: National Institute of Justice.
- Brodeur, J.P. and Shearing, C. (2005) 'Configuring Security and Justice', *European Journal of Criminology*, 2(4): 379–406.
- Button, M. (2002) *Private Policing*. Collumpton: Devon.
- Button, M. (2004) "'Softly, Softly", Private Security and the Policing of Corporate Space'. In Hopkins Burke, R. (ed.) *Hard Cop, Soft Cop: Dilemmas and Debates in Contemporary Policing*. Collumpton: Devon.
- Clarke, R.V.G. (2005) 'Seven Misconceptions of Situational Crime Prevention'. In Tilley, N. (ed.) *Handbook of Crime Prevention*. Collumpton: Devon.
- Collins, P., Corder, G. and Scarborough, K. (2005) *The ASIS Foundation Security Report: Scope and Emerging Trends*. Alexandria, US: ASIS International.
- De Waard, J. (1999) 'The Private Security Industry in International Perspective', *European Journal on Criminal Policy and Research*, 7(2): 143–74.
- Garland, D. (1996) 'The Limits of the Sovereign State: Strategies of Crime Control in Contemporary Society', *British Journal of Criminology*, 36(4): 445–71.
- George, B. and Button, M. (2000) *Private Security*. Leicester: Perpetuity Press.
- Gill, M. and Spriggs, A. (2005) *Assessing the Impact of CCTV*, Home Office Research Study number 292. London: Home Office. <http://www.homeoffice.gov.uk/rds/pdfs05/hors292.pdf>.
- Gill, M. and Hart, J. (1997) 'Policing as a Business: the Organisation and Structure of Private Investigation', *Policing and Society*, 7: 117–41.
- Gill, M.L. and Mawby, R.I. (1990a) *A Special Constable: A Study of the Police Reserve*. Aldershot: Avebury.
- Gill, M.L. and Mawby, R.I. (1990b) *Volunteers in the Criminal Justice System: A Comparative Study of Probation, Police and Victim Support*. Milton Keynes: Open University Press.
- Johnston, L. (2000) *Policing Britain: Risk, Security and Governance*. London: Routledge.
- Johnston, L. and Shearing, C. (2003) *Governing Security*. London: Routledge.
- Jones, T. and Newburn, T. (1998) *Private Security and Public Policing*. Oxford: Clarendon Press.
- King, M. and Prenzler, T. (2003) 'Private Inquiry Agents: Ethical Challenges and Accountability', *Security Journal*, 16(3): 7–18.
- Loader, I. (1997a) 'Thinking Normatively About Private Security', *Journal of Law and Society*, 24(3): 377–94.

- Loader, I. (1997b) 'Private Security and the Demand for Protection in Contemporary Britain', *Policing and Society*, 7: 143–62.
- Mawby, R. (2005) *From Police Science to the Science of Policing*. CEPOL police studies subgroup, Amsterdam, August.
- McLeod, R. (2002) *Parapolice: A Revolution in the Business of Law Enforcement*. Toronto: Boheme Press.
- Morgan, R. and Newburn, T. (1997) *The Future of Policing*. Oxford: Clarendon Press.
- Noakes, L. (2000) 'Private Cops on the Block: A Review of the Role of Private Security in Residential Communities', *Policing and Society*, 10: 143–61.
- Prenzler, T. (2004) 'The Privatization of Policing'. In Sarre, R. and Tomaino, J. (eds) *Key Issues in Criminal Justice*. Adelaide: Australian Humanities Press.
- Prenzler, T. and Sarre, R. (2002) 'The Policing Complex'. In Graycar, A. and Grabosky, P. (eds) *The Cambridge Handbook of Australian Criminology*. Melbourne: Cambridge University Press, 52–72.
- Rigakos, G. (2002) *The New Parapolice*. Toronto: University of Toronto Press.
- Sarre, R. (2005) 'Researching Private Policing: Challenges and Agendas for Researchers', *Security Journal*, 18(4): 18–31.
- Sarre, R. and Prenzler, T. (1999) 'The Regulation of Private Policing: Reviewing Mechanisms of Accountability', *Crime Prevention and Community Safety: An International Journal*, 1(3): 17–28.
- Sarre, R. and Prenzler, T. (2000) 'The Relationship Between Police and Private Security: Models and Future Directions', *International Journal of Comparative and Applied Criminal Justice*, 24(1): 91–113.
- Shearing, C. (1992) 'The Relation Between Public and Private Policing'. In Tonry, M. and Morris, N. (eds) *Modern Policing: An Annual Review of Research*. Chicago: University of Chicago Press, 15: 399–434.
- Welsh, B. and Farrington, D. (1999) 'Value for Money? A Review of the Costs and Benefits of Situational Prevention', *British Journal of Criminology*, 39(3): 345–68.
- Zedner, L. (2003) 'Too Much Security', *International Journal of the Sociology of Law*, 31(3): 155–84.

# Index

- Abele, J., 138  
access control, 8, 39, 92, 102–3, 108, 132–3, 591, 600, 604, 614, 625–6  
*Access Control Entries* (ACEs), 374  
*Access Control List* (ACL), 374  
biometric systems, 42, 109, 193, 354, 619, 624  
  identification card, 39  
  signature match, 625  
  smart card, 623  
  techniques, 354  
car parking revenue, 604  
in computer/network systems, 359, 367–8, 371–4, 378  
as a deterrent, 472  
devices, 93–4, 109, 221, 353, 488, 619  
methods of implementation, 103  
physical security measure, 611  
principles, 93  
smart card rapid response, 624  
symbolic and real barriers/methods of, 97, 100, 221, 274  
in WV risk reduction, 253  
Acousto-Magnetic (AM), Radio Frequency (RF), Electromagnetic, and Microwave, 469  
adversary attack, 82–4  
al-Qaeda Network, *see under* terrorism  
alarms, 37  
Aldo Moro, 348  
American Civil War, 35  
American ‘community oriented policing’ (COPS) strategy, 105, *see also under* police/policing  
American criminal justice system, 271  
American Federation of State County and Municipal Employees (AFSCME), 249  
American Hotel and Lodging Association, 129  
American intelligence history, prominent names in, 156  
American National Standards Institute (ANSI), 130  
American Revolution, 152  
American Society for Industrial Security (ASIS), 37, 125, 129, 139, 164, 165  
American Society for Testing and Materials (ASTM), 27, 130  
American Sociological Society, 203  
Anderson, R., 84, 376  
Angleton, J., 156  
Anti-Money Laundering, 262  
anti-terrorist efforts, 336, 339, *see also* terrorism, response to  
  al-Qaeda movement threat, 346–8  
  biometric systems, role of, 109–11  
  combating terrorist groups, private sector contributions, 352–4  
  conflict in Iraq damaging consequences of the, 336  
  crime maps, 110  
  effective strategy to dismantle the al-Qaeda network, 346–54  
  mass media, role of, 348–9  
  measures, 355  
  prerequisite for an effective strategy, 346  
  public support, tasks, 347–52  
  rights and wrongs of the invasion of Iraq, 336  
  terrorist finance, push against, 270  
  UK’s Joint Terrorism Analysis Centre (JTAC), 336  
  War Against Terrorism, 336, 339  
ANZUS, 334  
Architectural Liaison Officers (ALOs), 101  
  areas of training, 417  
Arts Plaza, 401  
Ashton, Kevin, 462, 480  
Association for Payment Clearing Services, 276  
Association of Certified Fraud Examiners (ACFE), 204, 206  
  2004 *Report to the Nation*, 206  
  first Report to the Nation on Occupational Fraud and Abuse, 206  
Association of Chief Police Officers (ACPO), 27, 565  
Atomic Energy Commission, 520  
Australian National Health and Medical Research Council (NHMRC), 248  
Auto ID Centre, 462  
  creation of the Electronic Product Code (EPC), 465  
  funding by major retailers, 465  
  network labs, 479

- MIT, University of Cambridge, University of Adelaide, Keio University, Fudan University, University of St Gallen, 479
- AXA group, 553
- Axelrod, A.D., 414
- Babney, D.A., 315
- Bakken, G., 138
- Bamfield, Joshua, xvi, 14, 485
- Bamford, J., 171
- Bank of Credit and Commerce International, 262, 277
- Bank of England, 26
- Bank Protection Act 1968, 165
- Barnard, R., 83
- Baron, R.A., 243
- Barr, R., 191
- Battle of Midway, 1942, 153
- Baumgartner, M.P., 214
- Bay of Pigs scandal, 1961, 151
- Beaver, K., 518
- Beccaria, C., 95
- Beck, Adrian, xvi, 14, 462
- Bell, Alexander Graham, 37
- Bell-LaPadula model, 373, 374
- Beng, X., 315
- Bennet, T., 295, 445, 447, 453
- Benson, M.L., 214
- Bertalanffi, L., 655
- Business Impact Analysis (BIA), 542–3
- Bichler-Robertson, G., 293
- Billings, R., 534
- biometric systems, *see under* anti-terrorist efforts; access control; terrorism, response to
- Black's Law Dictionary, 123
- Blake, W., 138
- Blakely, E.J., 94
- Block, C.R., 109
- Boutros-Ghali, Boutros, 47  
*An Agenda for Peace*, 47
- Bow Street Patrols/Runners, 31, *see also* police/policing
- Bowers, K.J., 289, 296
- Bowie, V., 231
- Bradley, W., 138
- Braithwaite, J., 272
- Brantingham, P.J., 107, 126, 312
- Brantingham, P.L., 107, 126
- Brink, W.P., 38, 39, 424
- British ALOs, 107
- British Chambers of Commerce (2002) report, 290
- British Chambers of Commerce (BCC), 297
- British Crime Survey (BCS), 283, 289
- British Home Office Research Unit's, 104
- British intelligence service, 171
- British Retail Consortium, 297
- British Security Industry Association (BSIA), the National Security Inspectorate (NSI), 27, 130
- British security services, 172
- British Standards Institution (BSI), 27
- British United Provident Association (BUPA), 179
- Brough, M., 387, 392–3
- Brown, D., 387, 392–3
- Buck, A., 289, 296
- Buckle, A., 313
- Buerger, M.E., 194
- Buikema, C., 576
- Burgess, E.W., 96
- burglars/burglary, *see* commercial burglary; domestic burglary
- Burns International Detective Agency, 163
- Bush, George W., 171, 334, 340
- Business Continuity Management (BCM), 14, 538–41  
applicability to wide range of events, 556  
identifying potential weaknesses, 14, 532  
potential risks from suppliers, 544  
structure, 532
- business frauds, *see* frauds/business frauds; financial crimes; white-collar crimes
- Business Impact Analysis (BIA), 541
- Business Impact Evaluation (BIE), 544
- Business Improved Districts (BIDs), 41
- Butler, G., 293, 295
- Button, Mark, xvi, 15, 563
- Cadbury-Schweppes, 548, 550
- Caime, G., 305
- Calder, James D., xvi, 11, 146
- Calder, W.D., 171
- Cameron, M.O., 308
- Campbell Collaboration, 442
- Canadian Corps of Commissionaires, 578
- Canadian Union of Public Employees (CUPE), 249
- Canter, D., 138
- Cardone, Caroline, xvii, 12, 302
- Carnegie Mellon University, 376
- Carneiro, R.L., 21
- Carrington, F., 138
- Carter, D., 55

- CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering), 477, 479
- CCTV, 90, 318, 386, 438–46, 448–58  
 ‘big brother’ effect, 453  
 civil liberties threats, 14, 441, 450–5  
 crime prevention measure, 454  
 effectiveness, 290, 442–3  
 help to the police, 447–8  
 impact on vehicle crime, 442  
 potential threat to privacy, 454  
 psychological deterrence, 222  
 reduced levels  
   of shoplifting, 453  
   vehicle crime in car parks, 444  
 regulations to guide use, 455  
 two major concerns, 438
- Cecil, J., 140
- Central and West Lancashire Chamber of Commerce and industry, 290
- Central Intelligence Agency (CIA), 151, 155, 157–8, 168–9, 171  
 analytical function, importance of, 157, 159, 162  
 centralized R & A branch, 147  
 Directorate of Intelligence (DI), 147, 169  
 role of, 151  
 Sherman Kent School for Intelligence Analysis, 168  
 and US bureaucracy, 154
- Central Intelligence Group, 151
- Central Saint Martins Design School in London, 189
- Centre of Criminology at the University of Toronto, 167
- CERT (computer emergency response team), 376, *see also under* computer (IT) security
- Chainey, S., 448, 450, 454
- Challinger, Dennis, xvii, 15, 586
- Chandler, Raymond, 433
- Chaney, J., 140
- Charman, E., 446, 453
- Charter of the Congress for New Urbanism, 102
- Checkland, D., 655
- China, 33, 34
- City States of Renaissance Italy, 42
- Civil War, 1861–65, 152, 162, 424
- Clark, J.P., 204, 208–9, 211, 213–15, 220  
*Theft By Employees*, 208
- Clarke, R.V., 98, 104, 188, 191, 223, 296
- Clinard, M.B., 203
- Clutterbuck, R., 60  
*Kidnap and Ransom: The Response*, 60  
*Kidnap, Hijack and Extortion: The Response*, 60
- Coalition Against Terrorism, The, 334
- Coca-Cola, 533, 542, 547, 551–6
- Code of Hammurabi, 121
- Confederation of European Security Services (COESS), 385, 399, 582
- Cohen, L.E., 105, 180, 210
- Cohen, M., 192
- Cold War, 45–6, 341  
 arbitrary equilibrium created, 46  
 ‘the balance of nuclear terror’, 46  
 Berlin Wall, breakdown, 46  
 end of the, 46  
 era of, 36, 45, 48  
 threat perception of, 56
- Coleman, A., 103
- Colquhoun, Patrick, 31
- commercial burglary, 289–90, 291–2, 295,  
*see also* domestic burglary  
 awareness campaign, need for, 297  
 burglar alarms, 288  
 comparisons with domestic burglary, 295  
 exploring patterns to, 292–3  
 extent of, 264–96  
 five research findings, 295  
 forcible entry, most common type of, 281  
 intruder alarms, 288  
 perceptions of different sub-groups, 284  
 reduction initiatives/proactive initiatives, 296  
 Hotel Burglary Reduction initiative, 289, 291  
*Industrial Watch*, 288  
*Small Business and Crime* initiative, 290  
*Safer Cities* programme, 288  
*Small Retailers in Deprived Areas* initiative, 288, 290–1  
 Small Business Strategy of the Safer Merseyside, 289  
 risks, 292  
 three sets of criteria, 296  
 Victim Support, 291
- Commercial Victimization Survey (CVS), 282
- computer (IT) security, 367, 371, *see also* cybercrime/cyber-security  
 -based mapping using GIS, 107  
 block cipher, deployment, 360, 364  
 computer crime, 40, 59, 203

- firewalls, applications of, 370
- logical access control, 372–4
- Orange Book, US Department of Defense, 371
- systemic measures to protect information and computer leaks, 59
- viruses, 40, 367
- vulnerabilities and attacks
  - Aleph One, 375
  - CERT web pages, details on, 376
  - Internet worm, 375
  - principle of least privilege, 376
  - variety of criminals, 40
- Concealable, Removable, Available, Enjoyable, and Disposable (CRAVED), 105, 305
- Congress of Vienna, 1815, 46, *see also* national versus corporate security
- Cooke, W., 37
- Cornish, D.B., 188, 209
- Cornwall Business Crime Survey (CBCS) 2001, 283
- corporate crimes, 203, 262–3, 261, 266, 270, *see also* financial crimes
  - apathy to victims, 287
  - 'blue-white collar crime', 263
  - capital flight and money-laundering, 262
  - corporate governance, strong focus on, 261
  - data security, 263
  - definition of, 204
  - differentiation between crimes, examples of, 262
  - financial crime risks, analytical perspectives on, 263–5
  - frauds, risk analysis of, 264
  - money laundering, 263, 266–70
  - neglect of financial crime, 262
  - risks from outsourcing, 263
  - white-collar and organized economic crimes, 261, 263, *see also* frauds/business frauds; white-collar crimes; financial crimes
- corporate security, 54, 57, 59–60, 137, 586, 592, 600, 602–3, 611
  - all staff, fulfill a security function, 15
  - assets needing protection, 611
  - bad corporate security, 595–7
  - corporate crime control, 270
  - corporation, definition of, 586
  - corporate management's view of, 588
  - cyber security, 45, *see also* computer (IT) security; cybercrime/cyber-security
  - EFTPOS facilities for customers, 605
  - embedding security in the corporation, 605
  - funding of, 600–1
  - future risk assessment activities, 593
  - global security function, new model for, 607
  - level of security, determinants of, 612
  - major failures, list of, 588
  - measuring value of, 598
  - measuring devices, 606
  - mainstays of, 599
  - management, 590
  - opportunity cost, definition of, 517
  - outsourcing considerations, 602
  - perceptions of invasion of employee privacy, 590
  - policy, 589
  - preventive impact, evaluation of, 599
  - prioritizing threats, 592
  - programs, 55
  - range of activities, 591
  - research, 53
  - role of, openly acknowledged, 587
  - return on investment (ROI), 517, 600
  - risk assessment process, 592–3, *see also* risk management
  - security management plan, 611
  - strategy for protection of assets, three components of, 612
  - three pillars, 607
  - training programs, 9
  - upgradation, 517
  - visibility of, 587
- Cortese, V., 386, 399, 402
- Covello, V., 77
- Coyle, R.G., 655
- Crampton, Jason, xvii, 13, 358
- Cressey, D., 203, 208
- Crime and Disorder Reduction Partnerships (CDRPs), 184, 290
- crime prevention, 104, 127, 148, 189, 190, 195, 220, 425, 469
  - aim of, 273
  - applications, 97–8, 100
  - appropriate situational preventive response, 187
  - benefit denial devices (BDDs), 222
  - boundary definition/markers, 100–2
  - costs of crime, 192
  - crime reduction initiatives, key prerequisites of, 287, 292
  - criminogenic environment, dealing with, 189
  - designing-out crime, 189–90

- crime prevention – *continued*
  - diffused and anticipatory benefits, 191–2
  - displacement and deflection, 190–1
  - electronic article surveillance (EAS)
    - systems, 222, *see also* EAS
  - five nodes, 193
  - good customer service, a deterrent, 16
  - historical background, 424
  - horizons of response, 148
  - and law enforcement, 424–5
  - market effects, 192
  - no crime remedy is forever, 195
  - preventive audit survey (PSA), 221
  - public-private partnership, 276
  - risk-focused crime prevention, 180–3
  - strategies, 408, 610
  - situational, techniques of, 182, *see also*
    - situational crime prevention
  - theory, practice, applications, 97–9
  - three major emphases, 410
  - three proactive steps, 221
- Crime Prevention Through Environmental Design (CPTED), 93, 97, 102–4, 189, 318, 612–13
  - application to target hardening, 610, 614
  - based security strategies, 103
  - crime prevention, three overlaying
    - strategies of, 613
  - crime theories, 104–5
  - evolution of design of built environment, 189, 613–14
  - natural access control, natural surveillance, 613
  - strategies, nine fundamental, 102
  - terrorism prevention, 110, *see also*
    - anti-terrorist efforts; terrorism,
    - response to
  - WV reduction, related to, 250
- crimes, 12, 181, 194–5
  - benefits of, 187
  - categories
    - blue-collar persistent offenders, 265
    - business people, 264
    - élites, 264
    - individuals, 265
    - professional criminals, 265
    - counterfeiting, 34
    - websites, hijacking/phishing, 265
  - crime control mainstream, 261
  - detection monitoring, 49
- Crime Liability Monthly, 121
- deception by agents/new technologies, 265
- foreseeability, 11, 127, *see also*
  - foreseeability
  - hotspots, 194
  - occupational crime, 204
  - repeat victimization, 193
  - technological advances, benefited from, 49
  - Type 1 UCR ‘index property crimes’, 206
- crimes and organizations, 203, 205–6, 222
  - employee theft and staff dishonesty, 203, 205–7
  - external threats e.g. shoplifting, 222
  - four primary sources, 206
  - inventory shrinkage, 206, *see also*
    - shrinkage/shrinkage reduction
  - ‘white collar crime’, 203, *see also*
    - white-collar crime
- criminal behavior, 97
  - causes of, 96, 111
  - criminogenic factors, 265
  - motivation for, 213
  - Sutherland’s theory, nine propositions, 215
  - ‘techniques of neutralization’, 216
- criminal justice, 179, 183, 355, 395, 424, 434, 630
  - criminal prosecution, symbolic
    - significance of, 271
  - effectiveness, 278
  - faster reaction time, 264
  - functions, 149
  - ineffectiveness, 102
  - policies, 270
  - suppression of al-Qaeda network, 340, *see also* terrorism
  - system costs, 184
  - system role, 347
- criminology/criminological, 12, 219
  - aspects of, 179–80
  - crime pollution theory, 183
    - categorization of approaches, 185
    - Goldstein’s hierarchy, 185
  - ‘crime science’, distinct discipline of, 12, 179
  - deterrence, two primary dimensions of, 219
  - displacement, intermediate notion of, 140
  - rational choice theory, 186
  - subdiscipline of victimology, study of, 135
  - tax breaks and incentives, 184
- crisis
  - definition, 534
  - three stages of, 536–7
  - typology, 541
- crisis management, 52, 543, 566
  - business impact evaluation (BIE), 544
  - defining characteristics of, 534–5

- description of, 533
- disaster management approach, 532
- effectiveness, 542
  - contingency/crisis plans, 555
  - frame of reference, 538
  - response, 556
- examples, 535, 547–56
  - case analysis of Perrier and Coca-Cola, 553
  - Coca-Cola contamination crisis, 551–3
  - Ford Explorer's tyres, 535
  - Perrier contamination crisis, 547–51
  - global continuity plan, absence of, 550
  - stakeholders 'primary' and 'secondary' groups, 542
  - supply chain analysis, interruptions in, 543–4
  - 'symbolism', 535
  - three stages of a crisis, 538
- Cromwell, P.F., 294, 311
- Crowe, T., 98
- cryptographic security
  - asymmetric algorithms, 360–3
  - cryptographic algorithms, 13, 359–60, 362, 364, 376, 378
  - cryptographic methods, 368
  - cryptosystems, asymmetric, 363
  - keyless algorithms, 360
  - roles and capabilities of the attacker, 362
- Culligan, J.J., 575
- Culver, R., 496
- Curtiss, J., 156, 171
- cybercrime/cyber-security, 182, *see also*
  - computer (IT) security
  - adversaries, insiders and outsiders, 80
  - applications, attacks, 85
  - cybercrime countermeasures, 40
  - cyber-systems, entry control, 83–4
  - outside threats, 80
  - response, semi-automation of, 82
  - threat types, 80
  - typical DBT statements for, 80
  - types of, 40
  - worms, severe threat posed by, 367
- Dabney, D., 314
- Dalton, D.R., 586, 588, 599, 602, 606
- Davies, S., 453
- Davis, Jason L., xvii, 12, 203
- Davis, M.G., 414
- design basis threat (DBT), 79, 82–5
  - evaluation of effectiveness, 87
  - identification of characteristics of, 81
  - sufficient information for design decisions, 80
- defense in depth (DID), 15, 610, 612–13, 615, 625
  - application of security technology, 15
  - security design, 610, *see also* security design
  - security functions, 613
  - target hardening and CPTED, 614
- de Waard, J., 384–5
- Decker, S., 449
- Dedicated Cheque and Plastic Crime Unit, 276
- Defense Advanced Research Projects Agency (DARPA), 83
- Defense Intelligence Agency (DIA), 57, 151
- Deng, X., 314–15
- Denial of Service (DoS), 358–9, 367
- denial techniques, 318, 320
- Design Council, The, 189
- di Beccaria, Cesare, 31
- Diffie, W., 362
- Dijk, J.J.M. Van, 284, 288
- DiLorenzo, R.L., 598
- Director of Central Intelligence (DCI), 157
- Director of National Intelligence (DNI), 157
- Directorate of Intelligence (DI), 157
- disaster management, *see under* crisis management
- displacement/deflection, 190, 274, 290, 336, 450, 466, 642
  - definition, 191
  - domino effect, 180
  - effects similar to, 192
  - fallouts of situational crime prevention, 312
- Distributed Denial of Service (DDoS), 367
- Ditton, J., 213, 440, 442–3, 445–6, 450, 454
- Dixon, J., 440, 447, 454
- Dombroff, M., 138
- domestic burglary, 294, *see also* commercial burglary
  - access through subterfuge, 281
  - alley-gating, reduction strategy, 293
  - emotional effect on victims, 287
  - fencing and disposal, 295
  - repeat victimization, 286
- domestic security, 148, 166
  - community, 149
  - domestic security, US
    - 1971 Rand Report on private security, 166
  - evidence-based approach and methodology, 148
  - Hallcrest Report, 167
  - linked to national defense, 166
  - management, 147

- domestic security – *continued*  
 measure the progress of, 170  
 organizations, 165  
 profession, 149  
 various forms of, 166
- domino effect, *see under*  
 displacement/deflection
- Donald, I., 294
- Donovan, William ‘Wild Bill’, 153–5
- Downes, D., 171, 156
- Drapeau, A.S., 493, 503
- Drucker, P., 502
- EASI (Estimate of Adversary Sequence Interruption), *see under* security systems, analysis
- Eck, J. E., 319, 414
- Economic and Social Council (ECOSOC), 47
- Efficient Consumer Response Europe, 479  
 collaboration between retailers and their suppliers, 479  
 ECR report: *Automatic Product Identification and Shrinkage: Scoping the Potential*, 479
- electronic article surveillance (EAS), 319, 598  
 barcode/tags, 463
- International Article Numbering Association (EAN International), 463
- source tagging  
 automatic billing, 480  
 cost considerations, 480  
 level of reliability, 473  
 visibility and deterrence, 473
- systems, false alarms, 472
- Uniform Code Council (UCC), 463
- Universal Product Code (UPC), 463
- Electronic Numerical Integrator and Computer (ENIAC), 40
- Elig, G., 576
- Elkind, T., 414
- Elliott, Dominic, xviii, 14, 532
- employee theft/dishonesty, *see also* retail crime; shoplifters/shoplifting  
 business failures, major proportion of, 12  
 criminal opportunities reduction, 223  
 ‘culture of dishonesty’, three categories, 207, 215  
 definition, 204  
 deterrence, two primary dimensions, 218  
 external economic pressures, 208–10  
 fallouts of, 207  
 guilt neutralizing techniques, 217  
 impact of location factors, 223  
 level of employee involved, 206, 214  
 limiting loss, four preventions, 220  
 nine factors considered before committing a crime, 209  
 non-criminal sanctions, 205  
 property deviance and production deviance, 205  
 rational choice theories, 207–8, 212, 312  
 reduce opportunity levels, 211  
 responses to, 220–3  
 routine activities/activity theory, 210,  
*see also* routine activities theory (RAT)  
 scale of, 209  
 social desirability, 211  
 surveillance, 318, *see also* surveillance  
 theft opportunities, 210  
 theft, a form of debt collection, 213  
 theories of, 207–8, 210–11, 212–15  
 three types of property, theft of, 218  
 two major forms of, 205  
 workplace deviance, 213–14
- English East India Company, 42
- Enron, 261
- entry control  
 equipment for authorized personnel, 528  
 technologies/systems, details of, 83–4  
 vetting for fraud, 274
- environmental criminology, 106, 126  
 analytic geometry/behavioral geography  
 of offender and offence occurrences, 107
- criminal behavior and social economic environments, 95
- security strategies  
 access control principles, 93  
 definitions, 90–1  
 environmental studies, future  
 directions of, 108  
 key points, 111–12  
 security design, environmental cues  
 and messages in, 93  
 site selection and layered defenses, 92
- Environmental Design Research Association (EDRA), 91
- EPC Global Inc, 465
- Erikson, B., 311, 394
- Escamilla, T., 83, 85
- EU Working Time Regulations and the National Minimum Wage, 398
- European Agency for Safety and Health at Work (EASHW), 249
- European Commission, 230

- Faigman, D., 137
- Farrell, Graham, xviii, 12, 179
- Farrington, D.P., 99, 313, 319, 442, 444, 599
- Fast Moving Consumer Goods sector (FMCG), 462, 479
- Fayol, H., 486
- Fed-OSHA, 248
- Federal Bureau of Investigation (FBI), 42, 57, 151
  - domestic law enforcement and intelligence roles, 151
  - Office of Intelligence, 168
- Federal Emergency Management Agency (FEMA), 92
- Felson, M., 105, 180, 182–3, 210
- Ferrara, J., 308
- Feuerverger, A., 413–14
- Feyerabend, P., 655
- Fielding, Henry, 31
- Figlio, R., 600
- Financial Action Task Force, 269, 275, 278
- financial crimes, 266, 276, *see also*
  - corporate crimes; frauds/business frauds; white-collar crimes
  - blue-collar frauds, 270
  - concern with 'macroeconomically relevant' phenomena, 262
  - forms of
    - bribery, 261
    - fraud, white-collar or blue-collar, 261–2, 272, *see also* white-collar crimes
    - mis-selling of financial services products, 261
    - money laundering, 263, 266
  - major fraud policing, two strategic directions, 271
  - manipulation of trust, 263
  - responses to, 148, 270–2
  - state role in protection, 272
- Fisher, Bonnie S., xviii, 12, 229
- Fisher, R.J., 511–12, 576
- Fitzgerald, K.J., 537
- flea markets, 479
- Flood, R.L., 655
- Focault, Michael, 451
- Follett, M., 486
- forensic criminology/science
  - broadest definition, 118
  - generic term for criminalistics, 118
  - predictor of future behavior is past behavior, 124
  - present and future scope, 119
  - and psychology, 124
- forensic security
  - evidence, forensic, 119
  - expert, 137
  - introduction to, 118
  - topics of concern for the, 137
  - and premises liability litigation, 120–3
  - specialists, 120, 129, 135
    - manage the defense of a lawsuit, 120
    - standards of care pertaining to security, 129
  - studies, 136
- foreseeability, 11, 123–9, 133, 136, 138, *see also under* crimes
  - balancing test, 128
  - definitions of, 123
  - elements in determining, 125
  - forensic point of view, 140
  - four tests of, 124, 139
  - General Security Risk Assessment, 125
  - issues impacting upon, 127
  - reasonable behavior, 129
  - relevant time frame, 125
  - special relationship and foreseeability, 129
  - specific harm test, 124
  - specific location of a property, 126
  - 'three-way' test of security adequacy, 128
  - threshold assessment, 128
  - totality of the circumstances test, 126–8
- Fosdick, R., 172
- Francies, D.B., 317
- Francis, J., 564
- frauds/business frauds, 7, 12–13, 204, 261, 264–6, *see also* financial crimes; white-collar crimes
  - arising out of transnational business expansion, 263
  - against companies, 273
  - blue-collar frauds, 270
  - and corruption, objectives and methods of prevention, 264
  - counterfeiting, 34–5, 265, 271, 475, 592
  - credit fraud, 277
  - Internet frauds, 49
  - major frauds, 262, 271
  - prevention and reduction, 270, 272
  - profile of perpetrators, 274
  - refund frauds, 415
  - telemarketing frauds, 273
  - vendor frauds, 206
- French, P., 496
- Frost and Sullivan, 623
- Gaffney, M.A., 292
- Galbraith, J., 488

- Galford, R., 493, 503  
 Garcia, Mary Lynn, xviii, 14, 509  
 Garrick, B.J., 512–13  
 Gartin, P.R., 194  
 Gelthsthorpe, L., 445, 447, 453  
 Geneva Convention, 340  
 geographic information systems (GIS), 90,  
   107–8, 110  
 George, Bruce, xix, 15, 563  
 Gerden, R., 578  
 Geyer, F., 655  
 Gandhi, Indira, 655  
 Ghone, G., 305  
 Gill, Martin, xix, 1, 438  
 global position radio-navigation system  
   (GPS), 90  
   technology, 108  
 Goldsmith, V., 138  
 Gotbaum, B., 402  
 Government Communications  
   Headquarters (GCHQ), 151  
 Gras, M.L., 451  
 Great Depression, 424  
 Green, G., 511–12  
 Greenberg, J., 213–14  
 Grillot, Suzette, xix, 11, 45  
 Grimshaw, R., 580  
 Groscup, 140  
 Group 4 Securitas and Securicor  
   (now merged into Group 4 Securicor),  
   36  
 group/team crime, 294, 307  
   offender profile, 294  
   organized retail crime, or ORC, 307  
   ram raiding, 294  
 Guthrie, R., 344
- Hackett, Sir John, 29  
 Hagan, F., 140  
 Haimes, Y.Y., 510  
 Hakim, S., 289, 292, 296  
 Hamil, W., 575  
 Hales, C., 486  
 Halibozek, E.P., 486, 489, 496, 591  
 Hall, E., 96  
 Hall, P., 94  
*Hallcrest Report*, 403, 425  
   national survey in the United States of  
   the views of police chiefs, 403  
 Hannagan, T., 493  
 Hardin, G., 533  
 Hargreaves, S.P., 655  
 Harriott, John, 31  
 Harris, D.K., 214
- Harrison, M., 374  
 Hart, James, 353  
 Hart, John, 344, 433  
 Hauser, J., 40  
 Hayes, Read, xix, 12–13, 302, 408  
 Hayman, S., 454  
 Health and Safety at Work Act 1974, 246  
 Health and Safety Executive (HSE) in  
   Britain, 231  
 Hearden, I., 294  
 Hellman, M., 362  
 Hemmens, C., 575  
 Hemming, M., 447–8  
 Henderson, C., 118  
 Henley, E.J., 510, 519  
 Hermann, C.F., 534  
 Hersey, P., 502  
 Hess, K., 512  
 Hillenkoetter, R.H., 154  
 Hillier, 101  
   ‘Space Syntax’ theory, 101  
 Hirschi, T., 274, 314  
 Hoffman, V.J., 394, 403  
 Hollinger, Richard C., xx, 12, 203  
 Holmes Edwin T., 37  
 Homant, R., 134, 138  
 Home Office crime reduction programme,  
   273  
 Homel, R., 127, 264  
 Homes, E.T., 37  
 Honess, T., 446, 453  
 Hoogenboom, R., 435  
 Hoover, J. Edgar, 42, 152, 154  
 Horning, D.N.M., 218  
 Horvath, F., 576  
 House, R.J., 503  
 ‘Huddersfield Crusade’ of the 19th century,  
   33  
 human intelligence (HUMINT), 56–7  
 Hummer, D., 403  
 Hyde, D., 569, 578
- Illuminating Engineering Society of North  
   America, 130  
 Inbau, F., 119  
 informal sector, 16, 42  
   called ‘dogs of war’, 42  
   Contemporary mercenaries, 42  
   organized protection rackets, 16  
   private military contractors, 42  
 information security management, 13, 149,  
   359, 377  
 Information Technology (IT), 37  
 Institut des Sciences, 385

- Institute of Management and Administration, 120
- Institute of Real Estate Management, 129
- Intelligarde International, 404
- intelligence, 56, 150–1, 153, 157, 160–7, 169–70  
 analysis, importance of, 154, 158, 161, 168  
 corporate intelligence gathering, 56  
 highly developed by the British, 151  
 human interpretation in, 161  
 Korean War surprises, 154  
 national and domestic security organizations, 170  
 R & A, 147  
 systems adequacy, oversight of, 146
- intelligence analysis and theory  
 construction, 156  
 Curtiss, Joseph, 156  
 Downes, Donald, 156  
 Knollenberg, Bernard, 156  
 Mendenhall, Thomas, 156  
 Pforzheimer, Walter, 156  
 Yale Library Project, 156
- intelligent CCTV, 619–21  
 Advanced Exterior Sensor (AES) system, 620  
 multiple video camera surveillance systems, 620  
 AMETHYST (AutoMatic Event auTHentication sYSTem) system, 621
- Institutional and Municipal Parking Congress, 130
- International Article Numbering Association (EAN International), 463, 465
- International Association for Healthcare Security and Safety, The, 130
- International Association of Campus Law Enforcement Administrators, 130
- International Association of Professional Security Consultants, 125
- International Commercial Crime Survey (ICCS), 236
- International Council of Nurses (ICN), 236
- International Council of Shopping Centers The, 129
- International Covenant of Economic, Social and Cultural Rights, 229
- International Crimes against Businesses Survey (ICBS) 1994, 282, 285, 292
- International Crime Victim Survey (ICVS), 281
- International Crime Victimization Survey, 234
- International Governmental Organizations (IGOs), 47
- International Institute of Security in 1968, 37
- International Labor Organization (ILO), 230
- International Monetary Fund (IMF), 262
- International Security of Security Management Association, 37
- Internet, 49, 265, 365, 375, 455
- Ireland, 32
- Irish Republic, 350
- Islamic terrorists, 516
- Jacobs, Jane, 102
- Jago, A.G., 503
- Janis, I.L., 495, 546
- Jefferson, T., 95, 580
- Jeffrey, C.R., 96, 102, 106
- Johansen, J.A., 655
- Johnson & Johnson, 479, 545, 555–6
- Johnston, L., 2–3, 285–7, 424, 580  
*The Rebirth of Private Policing*, 424
- Joint Combat and Tactical Simulation code (JCATS), 87
- Joint Military Intelligence College, 168
- Judge Learned Hand, 128
- Kahn, D., 171
- Kakabadse, A., 501
- Kakabadse, N., 501
- Kakalik, J.S., 397, 569, 576
- Kaplan, S., 512–13
- Katz, J., 310
- Kaufers, S., 140
- Kaye, D., 137
- Kennedy, Daniel B., xx, 11, 118
- Kennedy, John F., 151
- Kent, S., 156, 161
- Kitchen, T., 96
- Klemke, L.W., 308, 414
- Knollenberg, B., 156, 172
- Korean American Grocers Association, 250
- Kovacich, G.L., 486, 489, 496, 591
- Krafka, C., 140
- Kruissink, M., 293, 295
- Kuhlman, F., 344
- Kuhlman, R., 138
- Kumamoto, H., 510, 519
- Kyoto protocol, 184
- Labich, K., 502
- Langer, W., 156

- Langton, L., 505  
 Leclair, C., 578  
 Leonard, V.A., 172  
 Leven, Gustav, 547, 550, 554  
 Levi, Michael, xx, 12, 261  
 Licu, Elena, xx, 12, 229  
 Lim, B., 317  
 Lincoln, Abraham, 35  
 Loader, I., 9, 580  
 Lock Museum of America in Terryville,  
   Connecticut, 26  
 Lojek, C., 529  
 Lombroso, C., 95  
 Lomell, H.M., 441  
 Long, S., 578  
 loss prevention, 408, 417  
   display and design responses, 317–18  
   personnel, 119, 316–18, 412, 416  
   reduction, 320  
   strategy, 316  
   system techniques, 222  
 Loveday, K., 448–9  
 Lynch, 106  
 Lyon, D., 452
- Magill, C., 294  
 Maguire, M., 294  
 Makkai, T., 272  
 Mangione, T.W., 213  
 MANPAD attacks, 354  
 Manunta, Giovanni, xxi, 15, 629  
 Manunta, Roberto, xxi, 15, 629  
 Mars, G., 214  
 Massachusetts Institute of Technology, 40  
 Masuda, B., 221–2  
 Mattman, J., 140  
 Matza, D., 216, 311  
 Mawby, Rob I., xxi, 12, 281  
 May, D., 414  
 Mayhew, Henry, 303  
 Mayhew, P., 182  
 McCahill, M., 441, 449, 451–2  
   *The Surveillance Web*, 451–2  
 McCrie, F.M., 42  
   *Security Operation Management*, 42  
 McCrie, Robert D., xxi, 93, 11, 21  
 McDermid, V., 425  
 McGee, A., 582  
 McGoey, C., 138  
 McGuire, P., 138  
 McKay, H.D., 96  
 McLeod, R., 404  
 McManus, M., 403–4  
 Mellor, D.H., 655
- Mendenhall, T., 156, 171  
 Meredith, W., 541  
 Merton, R.K., 311  
 Metropolitan police (bobbies), 33, 42  
 Metropolitan Police Bill of 1829, 32  
 Metropolitan Police Vehicle Crime Unit, 276  
 Miccolis, J., 515  
 Michael, D., 395  
 Michigan Supreme Court, 124  
 Middle Ages, 25–6, 29  
 Miletich, D., 140  
 Military Information (later Intelligence)  
   Division, 152  
 Milken, M., 209  
 Miller, D., 537  
 Mintzberg, H., 486  
 Mirrlees-Black, C., 286  
 Mitchell, R.K., 535  
 Mitnick, K.D., 40  
 Mitroff, I.I., 537, 541–2  
 Moenssens, A., 118  
 Mollard, M.J., 578  
 Mollenkopf, J., 138  
 money laundering, 266–9  
   bank secrecy different forms, 269  
   conduits, 269  
   Financial Action Task Force, 269  
   international laundering, 268  
   legislative comprehensiveness, 267  
   light punishment, 266  
   major area of financial crime, 266  
   ‘offshore’ corporations, 269  
   offshore trusts, 269  
   perpetrators, profile of, 267  
   in property transactions, 267–8  
   retail service industries, 268  
   in services, 268  
   three factors of transformation, 267  
   three stages of a laundering cycle, 268  
   three-state process, 267  
 Moore, Richard, 308  
 Moro, A., 348  
 Morris, R.T., 40  
 Morris worm, computer worm, 40, *see also*  
   computer (IT) security  
 Muslim Coalition, 334
- Nalla, M.K., 394, 403  
 National Advisory Committee on Criminal  
   Justice Standards and Goals (1976),  
   167, 569  
 National Apartment Association, 129  
 National Approval Council for Security  
   Systems UK, 569

- National Association of Convenience Stores, 129
- National Association of Security Companies, 130
- National Center for the Analysis of Violent Crime (NCAVC), 250
- National Center for Injury Prevention and Control (NCIPC), 249
- National Center for Victims of Crime in Washington DC, 138  
quarterly magazine, *Victim Advocate*, 138
- National Council of Investigation and Security Services (1975), 37
- National Counterintelligence Officer for Economics, 55
- National Crime Prevention Council (2005), 41
- National Crime Victim Bar Association, 138
- National Crime Victimization Survey, 229
- National Fire Protection Association, 139  
'Guide for Premises Security' (NFPA 730), 139
- National Geospatial-Intelligence Agency, 171
- National Institute for Occupational Safety and Health (NIOSH), 249
- National Labor Relations Act of 1935, 163
- National Occupational Health and Safety Commission (NOHSC), 230, 249
- National Parking Association, 130
- National Police Library, Bramshill, England, 42
- National Security Agency (NSA), 151
- National Security Council (NSC), 147, 151, 169
- national security, 45, 54–5  
academics and corporations, diversity of approach, 55–6  
agencies, 58  
intelligence services, 12, 57, 147  
scholars, 53
- national security studies, academic journals  
*Contemporary Security Policy*, 52  
*Defense and Peace Economics*, 52  
*Defense and Security Analysis*, 52  
*Defense Studies*, 52  
*Intelligence and National Security*, 52  
*Journal of Security Studies*, 52  
*Security and Defense Review*, 52  
*Security Studies*, 52
- national versus corporate security, 45–6, 53
- National Violence Against Women, 229
- National Vocational Qualifications (NVQ), 401
- natural surveillance *see under* surveillance
- Naylor, R., 278
- network operations, 365  
Hypertext Transfer Protocol (HTTP), 365  
Internet Protocol (IP), 365  
Transport Control Protocol (TCP), 365
- network security  
confidentiality, 365  
countermeasures, 368  
DoS attack detection devices, 369  
Intrusion Prevention Systems (IPS), 371  
*Honeypots*, 371  
*Vulnerability scanning*, 371  
entity authentication/firewalls, 368  
security mechanisms  
secure channels, 368–9  
three popular approaches, 369  
*worms*, severe threat posed by, 367
- Nevada Supreme Court, The, 126
- New York City's Port Authority Bus Station, 183
- New York State Tenement House Commission, 95
- Newburn, T., 387, 392–3, 403, 454, 581
- Newman, J.H., 243
- Newman, O., 97, 101, 106
- Nordby, 119
- Norris, C., 449, 451
- Northern Alliance, 334
- Nuisance Alarm Rate (NAR), 83
- offence, types of, 12  
commercial burglary, 12  
household burglary, 12  
shop theft, 12  
white-collar crimes, 12
- Olson, J.N., 294
- Oppal, W.T., 578
- Osterburg, J., 137
- Outcalt, 303
- Oxnard Police Department, 250
- Painter, K., 99, 443
- Parfomak, P.W., 399, 401
- Paternoster, R., 209–10
- Paterson, Kenneth G., xxi, 13, 358
- Pauchant, T.C., 537
- Paulsen, D., 138
- Pearl Harbor, 1941, 163  
attack, 146  
tragedy, 153
- Pearson, N., 156
- Pease, Ken, xxii, 12, 179
- Peek-Asa, C., 251

- Peel, Robert, 32
- Perrier, 533, 542, 547–56
- Perrone, S., 285
- Pforzheimer, W., 156–71
- Phillips, C., 449
- physical security, 87, 521, 527
  - access/entry controls, 371–2, 527
  - analysing adversary actions, two techniques, 521
  - physical measures, historical evolution of, 22, 25–9
  - neutralization analysis, 87
  - systems, 520
- Pinkerton Agency, The, 35, 162–3, 424
- Pinkerton, A., 34, 162, 172
- Piper, Fred, xxii, 13, 358
- Piquero, N., 263
- police/policing, 4–12, 15, 27, 34, 42, 50, 80, 95, 101, 165, 250, 278, 303
  - business/corporate cooperation, 41, 353, 405, 435
  - CCTV, perceptions of, 440–56
  - community policing, 43, 105, 110, 291
  - costs, 102, 184
  - criticism of police services, 287
  - Evidence-Based Policing, 133
    - Hallcrest Report, US, 403
  - history of, 21–3, 33
  - hotel crime, 285–6, 289, 291
  - intelligence activities, 56
  - military nexus, 33
  - modern policing/technology
    - applications, 25, 29–32, 34, 103, 108
  - Oppal Commission of Inquiry, Canada, 578
  - private policing, 3, 99, 172, 402, 536, 563
  - private security personnel, 403, 405
  - proactive policing strategies,
    - development of, 271, 403, 405
  - ‘problem oriented policing’ approach, 104
  - public’s response, 347–8, 352, 355–6
  - risk of violence, 238
  - situational crime prevention, 104, 195
  - terrorist investigation, 337–8, 343, 346
- Police Reform Act 2002, 400
- Polygraph Protection Act 1988, 220
- Pope, A.R., 37
- post-Cold War world, 56
- post-World War II, 150, 424
- Potchak, M.C., 293
- Poulin, K., 132
- premises liability
  - absence of foreseeability, 123, *see also* foreseeability
  - concepts of foreseeability, breach of duty, causation, 122
  - ‘criminal profiling’, 134
  - individual deterrence, 134–5
  - litigation, 120 134, 136, 139
  - notion of ‘presumptive standards’, 132
  - offenders, four categories of, 134
  - risk sensitivity, eight variables of, 135
  - victimological theories, 136
- Prenzler, Tim, xxii, 13, 423
- President Karzai, 336, 342
- private investigators, 427, 434–5
  - A Suitable Job for a Woman: Inside the World of Women Private Eyes*, 425
  - categories of work, 427
  - contract security officers, 398
  - critical areas of law that relate, 431
  - cultural images, 433
  - deceptive tactics, 430
  - definitions, 423
  - difference between corporate and private clients, 429
  - earnings, 428
  - espionage, 49
  - ethics and conduct, 429–30
  - fictional private detective figures, 433
  - forms of malpractice, 429
  - integrity checks, 428
  - laws related to privacy, 433
  - legal powers and responsibilities, 431–3
  - limited regulation, 425
  - listening devices, 433
  - nature of work, 429
  - occupational licensing, 430
  - overlaps with a broader field, 423
  - regulation, main aims of, 430
  - regulation, 430–1
  - role of, 13, 426
  - skip tracing, 428
  - social impact, 434–5
  - special powers or rights, 431
  - traditional male domain, 425
  - work profile, 426–9
- ‘private justice’, growth of, 13, 434–5
- private security regulation, 58, 568–72, 573, 575, 577–81
  - analysis, information, methodology of collection, 563–4
  - definition of, 564
  - case against, 565–6
  - changing structure of policing, 581
  - Commonwealth Mutual Recognition Act 1992, 579
  - in North America/US, 575, 578

- licensing based upon character requirements, 579
- mandatory training standards, 578–9
- private policing alternatives, 288
- Private Security Case Law Reporter*, 121
- reflection of country's political structures, 566
- regional review, 571–80
- responsibility for regulation, three categories, 571
- Private Detective and Protection Activity in the Russian Federation*, 574
- three broad characteristics of comparison, 567
- training standards for armed security officers, 576
- Oppal Commission of Inquiry, Canada, 578
- National Security Competency Standards for Security Officers, Australia, 579
- plural model of regulation, 580
- 'private security', 34, 36
  - definitions of, 567
  - personnel training, 399
  - private, public, voluntary and informal, 3, 8
  - umbrella phase, 3
  - regulation of *see* private security regulation
- property deviance, *see under* employee theft/dishonesty
- product deviance, *see under* employee theft/dishonesty
- Protection from Harassment Act 1997, The, 246
- Public Interest Disclosure Act 1998, The, 275
- public security system, 29, 56, 96, *see also* police/policing
- Public Services International (PSI), 236
  
- Quayside Centre, 401
- Quinn, R.P., 213
- Quinney, R., 203
  
- radio frequency, 462–3
- Rapoport, A., 90
- Rasmussen, N.C., 522
- rational choice theories, 186, 208
- Radiological Dispersal Device (RDD), 343
- Reason, J.T., 537
- Redshaw, J., 286–7
- Reeve, A., 452
- Reith, C., 30
  - The Blind Eye of History* (1975), 30
  
- Renaissance, 29, 93
- retail crime, 408–9, *see also* employee theft/dishonesty; shoplifters/shoplifting economy, shoplifting's impact on, 321
- effective loss prevention, 409
- electronic article surveillance (EAS), *see* EAS
- environmental factors, 91
- situational crime prevention, 409
- source of data on employee levels
  - University of Florida's *National Retail Security Survey* (NRSS), 206
- retail security, 93
  - modern 'store-within-a-store' layouts, 93
- Reynolds, S., 537
- RFID, 14, 468, 474, 476–7
  - concerns about consumer privacy, 477–8
  - cost considerations, 476
  - EPOS systems, 480
  - general benefits of, 464–5
  - systems, three main components, 463,
- RFID tagging, 465, 478–9
  - developments in product identification, 463
  - item level tagging unlikely, 476
  - reducing the losses created by refund fraud, 474
  - role and challenges, 470–4
  - 'tagged world', 465
  - three level deterrent impact, 474
  - use of EAS, 468
  - versatility of, 464
- RFID/EAS, 469–70
- Rieple, A., 503
- Rigakos, G., 394–7, 404
- risk analysis, 77–9
  - assessment, 511, 512, 518–19, 524–5, 544–5
  - definition, 76
  - determination of uncertainties, 77
  - equation, 522–3
  - event tree and fault analysis, 79
  - identifying threats and vulnerabilities, 511
  - lifecycle, 523
  - optimizing asset protection, 78–9
  - principles of, 76
  - risk management alternatives, 511
  - situational crime prevention and CPTED, 110
  - system design criteria, 78
  - threat definition, 79
  - vulnerability assessments, 110
  - uncertainty, major element of risk, 519

- risk management, 14, 509–29, 538  
 answering a second set of questions, 513  
 effective incident management, key component of, 546  
 event trees and fault trees, 519
- River Police, 32
- Robinson, M., 138
- Robshaw, Matthew J.B., xxii, 13, 358
- Rogers, Bradley B., xxiii, 11, 66
- return on investment (ROI), *see under* corporate security
- Romm, N.R.A., 655
- routine activities theory (RAT), 186, 244, 312, 411, *see also* employee theft/dishonesty  
 application to ‘victimless crimes’, 183  
 crime patterns and trends, analysis of, 105, 183  
 description of, 105  
 how crime events occur, 181, 312  
 occurrence of crime, three factors, 210  
 requirements for crime occurrence, 181  
 three primary elements, 410
- Royal Society of Arts, 189
- Ruzzo, W., 374
- Saalman, H., 23  
*Medieval Cities*, 23
- Safe Haven Protection, 39
- Saferstein, R., 118, 137
- Saks, M., 137
- Samuels, R., 104
- Sanders, J., 137
- Sandia Corporation, 529
- Sandia methodology, *see* systems engineering/security systems engineering
- Sandia National Laboratories, 87, 510
- Sandoval, J., 529
- Sarno, C., 446
- Sarre, R., 581, 600
- Schneider, Richard H., xxiii, 11, 90
- Scottish Crime Survey, 285
- Scottish Security Association, 37
- Scottish Survey of Business Crime (SSBC), 283
- Secured by Design (SBD) housing, 101, 189
- Securitas, 36
- security, 1–3, 8–12, 21–2, 41, 66, 111  
 definition of, 91, 632–3  
 department, 493–4, 497, 499, 501  
 design, 94, 610  
 devices, 38–9, 42  
 different dimensions of, 489  
 effectiveness of, six priorities, 653  
 environment, 46–7, 49  
 fundamental principles of, 92  
 future analysis, 649  
 hazards, two types of, 510  
 history of, 21, 28, 32  
 methodology of, 651–2  
 risk assessment, 650, *see also* risk management  
 social role of, 10  
 theory, 9, 93, 111, 629–55, 630–1, 635–6, 639, 642, 645–6, 648  
 threats, 1, 45, 48, 80  
 Vulnerability, Opportunity, Capability and Intention, 648
- security audit, 368, 489  
 define the problem, 456  
 security gap, 492  
 two main features, 491
- Security Council of the United Nations, 47
- Security Industry Association, 37, 130
- Security Industry Authority, 400
- security litigation cases, 138–40
- security management, 36, 39, 66, 485–6, 486, 491, 494–5, 497, 504, 524  
 decision making, 66, 494, 515–17  
 implementation, control, feedback, 653  
 leadership, six characteristics of, 502–3  
 policy approaches, 95  
 principles of detection, 615  
 processes, three criteria, or limits, 642  
 products and services, 130–1  
 measures, 58–9  
 outsourcing, 263, 402, 405, 501–2  
 range of tasks, 485  
 risk assessment, 511, 514, 516, *see also* security risk management  
 strategy, 612, *see also* security strategies  
 structure, 497–501  
 systems, *see* security systems; security technology  
 technology, *see* security systems; security technology  
 theoretical principles, 612
- security manager, 40, 70, 66, 296, 476, 488, 490, 503  
 engineering principles for, 66  
 leads in codes of conduct, 503  
 optimal reporting relationship, 496
- security officer, 134, 385, 387–96, 399, 402, 501  
 preventing crime and anti-social behavior, 392  
 responding to problems, 386  
 working conditions, 397–8

- security risk management, 511
  - assessment, 14, 519, 592
  - consequence analysis, 523
  - definitions, 509–13
  - threat perceptions, treatment of, 517
- security strategies, 491
  - Balanced Scorecard, 492
  - notion of civitas, definition, 94
  - 'Security Business Plan', 491, 493
- security studies, national and corporate, 51–60
- security systems, 11, 66, 75–6, 83, *see also* security technology
  - active delay elements, 84, 528
  - analysis, 8, 86–7
  - characteristics of a well designed system, 68–75
  - components, 82, 653
  - continuous feedback, 73
  - design, basic principles of, 71–2, 81–2, 85, 87–8
  - definition of a complex system, 67
  - detection, delay and response elements, 81
  - determination of objectives, 87
  - digital signatures, 362
  - effectiveness of, 528
  - evaluation of, 86
  - electronic systems, 386
  - engineering, 72–4
  - goals/purpose of, 72, 527
  - intrusion detection elements, 83
  - physical, cyber- or executive protection, 526
  - probabilities, 76
  - response effectiveness, key indicator of, 528
  - Sandia Methodology, 72–3
  - scope, clear definition of, 15, 72
- security technology, 621–4
  - analysis frameworks, 15
  - appropriate technology, determinants of, 613
  - appropriate technology, instances of detection, 26, 614
  - detection systems, trends in, 623–5
    - AMETHYST and VMD compared, 621
    - barrier and open ground detection systems, 623
    - biometric-smart card interface, 623–4
    - hierarchy of intrusion types, 617–18
    - intelligent CCTV with charged couple device (CCD) cameras, 621
    - near infrared spectroscopy (NIRS)
      - application of, 622
    - sensor systems can include, 623
    - organizational assets for protection, 611, 615
  - security strategy, components of, 614
    - see also* security strategies
  - systems engineering, development trends
    - of, 66, 610; *see also* security systems; systems engineering
- September 11, 2001 (9/11), 13, 45, 51–2, 59–60, 100, 262, 329, 341, 440, 543, 592, *see also* terrorism; terrorist attacks
- Serious Fraud Office cases UK, 271
- Service Employees International Union (SEIU), 249
- sexual harassment at work, 231–2, 236–8, 241, 245, *see also under* workplace violence (WV)
  - associated anxiety, depression, 240
  - research in reduction of, 249
  - younger in age, 242
- Shaloo, J.P., 166, 172
- Shapiro, S., 263, 272
- Shapland, J., 223, 404
- Shaw, C.R., 96
- Shearing, C.D., 2–3, 15, 386, 394, 398, 400, 414, 563, 578, 580
- Sherman, L.W., 194
- ship crime, research into, 504
- Shipman, H., 536
- shop theft, 302, 305–7, 469, 477
  - definition, scope and scale, 302–3
  - response to, 315–16, 472
  - successful loss prevention efforts, 315
  - tag visibility and deterrence, 473
- Shoplifters Alternative/Anonymous, 321
- shoplifters/shoplifting, 304, *see also* employee theft/dishonesty; retail crime; shop theft
  - apprehension reports, self-report data, 313
  - benefit denial (BD), 320
  - building and store configuration, 91
  - CRAVED (Concealable, Removable, Available, Valuable, Enjoyable and Disposable), 305
  - deterrents research on, 316
  - five major motivation categories, 310
  - five subgroups, 308
  - four most-likely types, 309
  - impact of, 303
  - merchandise-based classification, 308
  - organized retail crime (ORC), 307

- shoplifters/shoplifting – *continued*  
 retailer response to, 315, 318–19, 320–1  
 cables and protective display fixtures, 318  
 Counseling/Rehabilitation, 321  
 effective shoplifting control, 315  
 electronic tags, 319, 473, 477, *see also*  
 EAS  
 mechanical response, 318–19  
 societal responses, 321  
 six main points of study, 323  
 theories of, 310–11  
 typology of, five categories, 308
- Short, E., 443, 450
- shrinkage/shrinkage reduction, 303, 462,  
 598, *see also* shop theft;  
 shoplifters/shoplifting  
 definition, 466  
 failures, key elements for, 467  
 in retailing, 466–70  
 levels of, 222  
 management, 473–4  
 problem of, 466–70, 477  
 ‘philosophy’, 478  
 responding to, 468–70  
 ‘Stock Loss Reduction Road Map’, 478  
 sweep thefts, two ways of response, 473,  
 475  
 two types: malicious and non-malicious,  
 466–7
- Shrivastava, P., 537, 541, 542
- Simpson, S., 209–10, 263
- Sipika, C., 538
- situational crime prevention, 25, 105–6  
 concept of, 220  
 framework, 312  
 objectives and methods of prevention, 264  
 rational choice and routine activity  
 theories, 105, 106  
 revisionist, 264  
 techniques of, 188, 312
- Sloan, Stephen, xxiii, 11, 45
- Smith, Clifton, xxiii, 15, 610
- Soviet bloc, 36
- Soviet Union, 45
- Spanish Trade Union Confederation of  
 Workers’ Commissions (CC.OO.), 249
- specialized journals  
 associated with terrorism, 53  
*Conflict Quarterly*, 53  
*Security Studies*, 53  
*Studies in Conflict and Terrorism*, 53  
*Terrorism and Political Violence*, 53  
*The Journal of Conflict and Law  
 Enforcement*, 53  
 focusing on corporate security  
*Security Journal*, 53
- Spitzer, E., 271
- Spriggs, A., 444–6, 450, 454
- Secure Shell (SSH), 369
- Secure Sockets Layer (SSL), 369
- standards movement  
 Underwriters Laboratories (UL), 27  
 Continent, 27  
 European Fire and Security Group, 27  
 Eurosafe, 27
- Stapley, Craig, xxiv, 11, 45
- Starrs, J., 118
- Stenning, P.C., 393, 563, 578
- Stilwell, Joseph, 164
- Stimson, Henry L., 153
- stock loss, *see also* shrinkage/shrinkage  
 reduction  
 indirect shrinkage, 475, *see also*  
 shrinkage/shrinkage reduction  
 management, 474–5  
 practitioners, 478  
 problem of, 462  
 strategic approach development, 475  
 two key areas, 475
- Stone, D.G., 209
- store detectives, 408, 417–18, *see also*  
 shoplifters/shoplifting; shop theft  
 emphasis on shoplifting suppression,  
 413  
 innovativeness, discipline and mental  
 toughness, 419  
 job, five primary domains, 415  
 responsibilities, 410, 412, 416  
 role, 412–14  
 tactical role of, 412–13
- Strategies Intelligence for American World  
 Policy*, 156
- Sun-Tzu, 29
- surveillance, 13, 34, 58, 85, 103, 109, 182,  
 269, 288, 426, 451–3, 599  
 biometric/electronic, 193, 222, 319  
 CCTV, 393, 410–11, 451–2  
 of criminals, 416  
 defensible space, three design elements  
 of, 97–9  
 detection, identification, and  
 observation, 622  
 of employees, 318  
 facilitators, 70, 99–100, 183, 320  
 formal, 98, 292, 297, 411  
 intelligence related, 156  
 natural, 97–9, 103, 288, 297, 613–14  
 organized, 98–9, 103

- visual, three main theoretical approaches, 451
- Sutherland, G., 538
- Sykes, G.M., 216, 311
- systems engineering/security systems
  - engineering, 66, 72, 79
  - asset identification/prioritization, 76, 78
  - definition, 67
  - deterministic analytic tools, 86
  - objectives, 72
  - principles of, 81, 87
  - Sandia methodology, 72–3, *see also*
    - Sandia Corporation; Sandia National Laboratories
- Talley, L., 138
- Tarantino, J., 138
- target hardening, 188, 599, *see also under*
  - CPTED; DiD; security design; security
- Tennessee Supreme Court, 128
- Terlouw, G.J., 284, 288
- terror wars, 340–1, *see also* terrorism;
  - terrorist attacks
- terrorism, 46, 48, 111, 329, 329–30, 332, 339–40, 342–6
  - al-Qaeda Network
    - assessment of, 334
    - cracks in, 337
    - effective strategy to dismantle, 13
    - movement, 342
  - as a long-term threat, 52
  - corrigible/incorrigible terrorism, 331
  - counter-terrorism, 109
  - emergence of ‘non-territorial terrorism’, 48
  - failure as a weapon, 333
  - foreign policy as a *chase gardé*, 355
  - future of, 341–4
  - international terrorism, 111, 329–31, 337, 342
  - introduction, 328–30
  - key statutory definition of, 329–30
  - liberal democratic response, general
    - principles of, 344
  - prevention/deterrence, 110, 337, 356
  - response to mass-casualty terrorist attack, 356
  - risks, 261
  - strategic impact of, 332–3
  - targeted acts of, 592
  - threats, 45, 91
- Terrorism Act (2000) UK, 329
- terrorist attacks, 337–8, 513
  - 7th July attacks, three aspects of, 338
  - assassination of Van Gogh, fallout of, 337
  - defeat of, major policy options for, 349
  - events of 9/11, 45, 262, 329, 333–6, 340–1, 352, 355–6, 513, 517, 524, 537, 592–3, 606
  - having a major strategic impact, 333
  - ‘holy war’, 335
  - Jihad, 342
  - London bombings, 337
  - Madrid train bombings, 513
- terrorist groups
  - al-Qaeda threat, 54
  - Aum Shinrikyo, 51
  - categories, 331
  - Cold War era, 48
  - communication in anonymity, 49
  - Sendaro Luminoso, 49
  - strategy, crucial flaw in, 348
  - targets, 50, 523
  - technologically savvy, 49
- terrorism, response to, 110, 328, *see also*
  - anti-terrorist efforts
  - 9/11 Commission Report, 334
  - biometric systems, role of, 109–11
  - characteristics of, 328
  - media’s role in frustrating terrorist aims, 348
  - Terrorism: Documents of Local International Control 1979–2005*, 329
  - terrorist attack response, devices, 109
  - Terrorist Threat Integration Center, 58
  - ‘traditional’ terrorist movements, 332
  - UN Security Council Resolution 1566, 329, 334
  - US Code Title 22 Section 2656f (d), 330
  - War Against Terrorism, 334
  - War on Terrorism, 332
- Terrorist Threat Integration Center, 58
- terrorists/international terrorists at large, 335
  - Abu Musab al Zarqawi, 335
  - Aymanalawahiri, 335
  - Osama bin Laden, 335
  - Saif al-Adel, 335
  - Sheikh Said, 335
- The Internet Engineering Task Force (IETF), 366
  - Requests For Comments (RFCs), 366
- theft/thieves, 211–12, 312, 409, *see also*
  - shop theft; shoplifters/shoplifting
- Thurman, Q., 311
- Tilley, N., 286, 287, 443

- Treaty of Westphalia 1648, 46  
 Trompenaars, F., 504  
 Truman, Harry, 154  
 Tucker, J., 214  
 Turnbull Report (1999), 538  
 Turner, B., 534, 536–7  
 Twin Towers attack, 146, *see also* terrorist attacks
- Uniform Crime Reporting Program (UCR), 206  
 UK Data Protection Act, 478  
 UK Department of Trade and Industry, 261, 270  
   (now disbanded) Crime Foresight Panel (2000), 261  
 UK's Crime and Disorder Act 1998, 184  
 Ullman, J., 374  
 UN, 47, 233, 334, 341  
   *International Covenant on Economic, Social and Cultural Rights* (1966), 247  
 UN General Assembly, the *Convention on the Elimination of All Forms of Discrimination against Women* (CEDAW) (1979), 247  
 Underwriter's Laboratories (UL), 130  
 UNI-Europa, 385, 399  
 Uniform Code Council (UCC), *see under* EAS  
 Universal Product Code (UPC), *see under* EAS  
 United Federation of Teachers, 249  
 United Kingdom, 26, 131  
 United Nations in 1948, 41  
   *Universal Declaration of Human Rights of*, 41  
 United States Post Office, 35  
 United States, 26, 273  
 US Army Map Service (later Defense Mapping Agency), 171  
 US Business Roundtable Survey of 100 American CEOs, 45  
 US Congress, 146  
 US Defense Intelligence Agency, 149  
 US Department of Energy (DOE), 520  
 US Department of Homeland Security, 92, 146  
 US Department of Justice, 319  
 US National Crime Prevention Council, 103  
 US Sarbanes-Oxley Act, 2002, 261  
 US Securities and Exchange Commission, 277
- Van Gogh, T., 337  
 vandalism, 285  
 Varoufakis, Y., 655  
 Vaughan, D., 218  
 Vertinsky, I., 546  
 Victim Support, 287  
 victim/offender relationships, 264  
 'victimless' crimes, 183, 264  
 victimology, 283  
   causation, alternative theories of, 135  
   second CVS, 285, 287–8  
 'violence in the workplace', 230, 240, 241, 246  
 vulnerability assessment (VA), 110, 139, 509, 512–13, 526–9, *see also* risk management  
   decision making requirement, 522  
   definition, 526  
   security system, identifying threat to, 523–5
- Wakefield, Alison, xxiv, 13, 383  
 Walsh, D., 293, 295  
 Walsingham, Sir Francis, 171  
 War on Drugs, 270  
 Washington, George, 152  
 weapons of mass destruction (WMD), 51, 46, 59, 340, 343  
 West India Company, 31  
 West, N., 171  
 Wheatstone, C., 18, 36, 37  
 white-collar crimes, 12, 271, *see also* financial crimes; frauds/business frauds  
   collective business action, 148  
   combating/control of, 261, 270, 276  
   criminal, profile of, 263  
   definitional discussion, 263  
   role of preventing, 261  
   schemes, 148
- Wickersham Crime Commission 1930, 166  
 Wiersma, E., 295  
 Wildhorn, S., 397, 569, 576  
 Wilkinson, Paul, xxiv, 13, 328  
 Wisconsin Marine and Fire Insurance Company of Chicago, 34  
 Wolfe, Tom, 271  
   *Bonfire of the Vanities*, 271  
 Wolfgang, M., 135  
 Woolworth, F.W., 304, 408  
 workplace deviance, *see under* employee theft/dishonesty  
 Workplace Health and Safety Act 1995, 246

- workplace violence (WV), 229, 238–43,  
241–2, 247, 252, 254
- classification of, three types, 231
- collaborative efforts to reduce, 250
- Crime Prevention through Environment  
Design (CPTED) model, 250, *see also*  
CPTED
- definition of work/workplace, 234
- definitions of concepts, 230–3
- domestic violence, 232
- employee-initiated violence, 232
- environmental control features, 250
- extent and nature of, 234–9, 254
- five organizational characteristics, 243–4
- four issues, 233
- four primary sources of, 234
- four types of, 231
- gender discrimination, 238
- guidelines for employers and employees,  
247
- human rights violation, 229
- ILO Declaration on Fundamental  
Principles and Rights at Work* (1998),  
247
- impact and costs of, 239
- intangible cost to organizations, 240
- international agencies collecting data,  
249
- international perspective is presented,  
234
- measurement efforts
- British Crime Survey (BCS), 233
  - Bureau of Labor Statistics (BLS)  
National Census for Fatal  
Occupational Injuries, 233
  - European Survey on Working  
Conditions, 233
  - International Crime Victimization  
Survey (ICVS), 233
- international sources of WV, 233
- National Traumatic Occupational  
Fatalities (NTOF), 233
- prevention/prevention strategies, 246–7,  
251–2
- effectiveness of prevention programs and  
polices, 254
- efforts to prevent, 251
- legislative and regulatory approaches to,  
245
- periodical review of policies/practices,  
253
- trade union efforts to reduce, 249
- work practices, 253
- a recognized hazard, 248
- research and data collection efforts
- Australian Work-Related Fatalities  
Studies, 239
  - National Crime Victimization Survey  
(NCVS), 233
  - National Institute for Occupational  
Safety and Health, 238
  - National Occupational Health and Safety  
Commission (NOHSC), 230, 249
  - National Traumatic Occupational  
Fatalities, 238
  - US Department of Labor's  
Occupational Safety and Health  
Administration (Fed-OSHA), 247
  - Washington Industrial Safety and  
Health Service Agency, 245
- research, methodologically weak, 241
- response
- four initiatives, 245
  - guidelines complementing legislation,  
248
  - recommendations, 252–3
  - risk factors, 244, 252
  - sexual harassment at work, *see* sexual  
harassment
  - stress resulting from, 241
  - typology, 'three-types', 231
  - workplace/work-related homicide, 233,  
238
  - victims attributes, 242
- World Health Organization (WHO), 236
- World Trade Center, 110
- World War II, 304, 147, 153–4, 165, 386
- Wroblewski, H., 512
- Wyss, G., 529
- Yates, A., 588, 593, 606
- Zedner, L., 9, 595
- Zimmer, F., 549