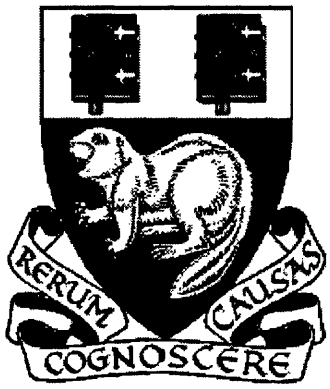
The Hunt for the Paper Tiger:

The Social Construction of Cyberterrorism



Sarah EH Thatcher

Department of Information Systems

London School of Economics and Political Science

Thesis submitted for the degree of Doctor of Philosophy

October 2006

ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106-1346

DECLARATION

I declare that the work presented in this thesis is my own.

Sarah EH Thatcher

Department of Information Systems

London School of Economics and Political Science

ABSTRACT

For two decades, there has been a high-profile debate on the issue of cyberterrorism. Politicians, law enforcement agents, the information security industry, other experts and the press have all made claims about the threats to and vulnerabilities in our society, who is responsible and what should be done.

This is a UK study in the field of Information Systems based on interpretative philosophical assumptions. The framework for the study is provided by the concept of moral panic, propounded by Cohen (2002) and elaborated by Goode and Ben-Yehuda (1994) and Critcher (2003). Moral panic is used widely in the reference discipline of Sociology as a tool for investigating the social construction of social problems in cases where there is heightened public concern and intense media interest, closely followed by changes in legislation and social control mechanisms. This study employs moral panic as an heuristic device to assist in the investigation of the social mechanisms at work in the social construction of cyberterrorism.

The corpus of data for analysis comprised articles from the UK national press relevant to cyberterrorism. A grounded theory approach was used to analyse these articles in order to identify images, orientations, stereotypes and symbolisation and to examine representational trends over time. Reflexivity in such a task is of the utmost importance, and the analytic process leading to an explanation of the social processes at work was deliberately divorced from the moral panic framework in order to guarantee rigour in the findings.

The findings set out an explanation of how the concept of cyberterrorism has been constructed over two decades and compares this explanation with a framework provided by a model of moral panic. These findings are then linked to wider issues about national security, civil liberties and state control of information and communication technologies.

TABLE OF CONTENTS

Declaration 2

Abstract 3

Table of Contents 4

Table of Figures 10

Dedication 12

Acknowledgements 13

Section I: The Foundations 14

Chapter 1 Introduction 15

1. The research question 15

2. Research approach and the Information Systems discipline 18

Chapter 2 Cyberterrorism in the Literature 21

1. Overview 21

2. Definitions of cyberterrorism 22

2.1 Netwar 22

2.2 Information warfare 24

2.3 Cyberterrorism 25

2.4 Definition of cyberterrorism adopted in this study 31

3. Who are the cyberterrorists? 32

4. Terrorist exploitation of ICTs 34

5. The risks from cyberterrorism 36

6. Risks and response: the information security perspective 44

7. The institutional response 48

7.1 National challenges 49

7.2 The challenge of public-private relationships 56

7.3 International challenges 60

8. The public response 62

9. Social reaction to cyberterrorism and the power of definition 64

Chapter 3 Moral panic: defining deviance 67

1. Introduction 67

2. Moral panic: an overview 67

2.1 A process of definition and action 68

2.2 Marking the moral boundaries 69

2.3 The underlying discourse 70

3. Cohen: the processual model 72

3.1 Emergence 75

3.2 Media inventory 75

3.3 Moral entrepreneurs/claims-makers 76

3.4 Experts 76

3.5 Elite consensus and concern, lack of organised opposition 76

3.6 Coping and resolution 77

3.7 Fade away 77

3.8 Legacy 77

4. Goode & Ben-Yehuda: the attributional model 77

4.1 Concern 78

4.2 Hostility 78

4.3 Consensus 79

4.4 Disproportionality 79

4.5 Volatility 80

4.6 Claims-makers 81

5. Moral panic and cyberterrorism 82

Chapter 4 Methodology and Research Design 84

1. Philosophical foundations 84

2. Research design 91

2.1 Summary 91

2.2 Corpus collection 92

2.3 Corpus analysis 96

Section II: The Findings 104

Chapter 5 Bringing the debate to the public: the UK national press 106

1. Setting the agenda: the association of hacking and terrorism 106

1.1 Cybercrime 112

1.2 Conventional terrorism 114

1.3 Cyberterrorism 114

1.4 Conventional crime 115

1.5 Communication 116

1.6 Crime: digital tool, conventional target 116

1.7 Information warfare 117

2. Image transmission: reporting the claims about hacking and terrorism 119

3. The press as claims-maker 122

Summary 126

Chapter 6 Concern, consensus and the claims-makers 128

1. Introduction: Concern and consensus 128

2. Politicians 132

2.1 Fostering concern 135

2.2 Politicians as claims-makers 137

Summary 142

3. Police and security services 143

3.1 Concerns 145

3.2 The international effort 151

Summary 153

4. The information security industry 154

4.1 Cyberterrorism as threat 157

4.2 Cyberterrorism as distraction 160

Summary 164

5. The rôle of experts 165

Summary 173

Chapter 7 Hostility and consensus 174

1. Hackers 176

2. The terrorist link 186

3. Demonisation of the technology 194

Summary 202

Chapter 8 Disproportionality and Volatility 204

1. Disproportionality 204

1.1 Source of attack 206

1.2 Method of attack 213

1.3 Target of attack 217

1.4 Outcome of attack 218

1.5 Reaction to attack 220

Summary 232

2. Volatility 233

Section III: The Finishing 235

Chapter 9 Discussion and Conclusions 236

1. Recapping the attributional model 236

1.1 Concern 236

1.2 Hostility 236

1.3 Consensus 236

1.4 Disproportionality 237

1.5 Volatility 237

1.6 Claims-makers 237

2. Emergence 238

3. Media inventory 241

3.1 Sensitisation 241

3.2 Stereotypes and folk devils 242

3.3 Exaggeration/distortion, symbolisation and prediction 245

4. Claims-makers 247

4.1 Orientations 248
4.2 Images 250
4.3 Causal explanations 252
4.4 Interests and exploitation 252
5. Experts 255
6. Elite consensus and concern 256
7. Coping and resolution 258
8. Fade away 262
9. Legacy 263

Chapter 10 Contributions and Future Directions 266

Appendix The Use of Atlas/ti 273

References 284

TABLE OF FIGURES

Figure 1 Frequency of UK national newspaper articles citing hacking and terrorism, by year 107

Figure 2 Frequency of UK national newspaper articles citing hacking and terrorism by quarter, with 8 quarter moving average trendline 107

Figure 3 Frequency of UK national newspaper articles citing hacking and terrorism and articles citing hacking only, by year 108

Figure 4 Ratio of number of articles citing hacking and terrorism to articles on hacking by year, with a 4 period moving average 108

Figure 5 Frequency distributions for categories of 'terrorism', 'crime' and 'miscellaneous' which are further broken down in Figure 6 111

Figure 6 Frequency distributions for non-exclusive behaviour categories described in articles citing hacking and terrorism 111

Figure 7 Frequency distributions for non-exclusive source categories for articles associating hacking and terrorism 120

Figure 8 Aggregate frequency distributions for sources influencing an article as a whole and for sources quoted or referenced specifically in the text 122

Figure 9 Frequency distributions of claims-makers' references to behaviour categories 129

Figure 10 Recurring themes referred to by different claims-makers 130

Figure 11 Frequency distributions for use of specific rhetorical mechanisms found to be significant in the corpus 131

Figure 12 Frequency distributions of rhetorical mechanisms used by claims-makers 132

Figure 13 Number of quotes from information security industry by year 155

Figure 14 Cumulative frequency distribution of *hacker* sub-codes by time 177

Figure 15 Relative importance of *hacker* sub-codes: sub-codes as a percentage of total *hacker* primary codes for each time period 178

Figure 16 List of character/appearance qualities attributed to hackers 185

Figure 17 Cumulative frequency distribution of *terrorist link* sub-codes by time... 187

Figure 18 Relative importance of *terrorist link* sub-codes: sub-codes as a percentage of total *terrorist link* primary codes for each time period..... 188

Figure 19 Cumulative frequency distribution of *technology* sub-codes by time 195

Figure 20 Relative importance of *technology* sub-codes: sub-codes as a percentage of total *technology* super-codes for each time period..... 196

Figure 21 Anatomy of a cyberterror attack 206

Figure 22 The concept of net-widening..... 208

DEDICATION

For Granddad, Crispin and Tommy

ACKNOWLEDGEMENTS

To my Granddad, who Believed and kept on asking when I would finish, so I did. You may now call me "Sir" and I'll join you in Class 4 (because there's no Class 5).

To Crispin, whose sweet nature, patience and generosity are without equal. I thank Goodness that debts have no currency between husband and wife, since this is one I shall never be able to pay off. You are, and always will be, my life.

To Tommy, who sat patiently by my side whilst I wrote this and gave his unconditional love and support as only a truly special dog can. My soulmate, losing you has left me desolate.

To Nancy, who made me laugh, against the odds, and was Beautiful throughout.

To Zak, who had big boots to fill, but got down to the job of being Gorgeous without preamble.

To Jasper, who is clearly Ridiculous and sings most beautifully; who also took up where the Brown One left off, although he did so from the comfort of the sofa.

To Alice the Gimp, Bunty the Basher, Camilla (RIP), Dora the Explorer, Scrawny Elsie and Freda the Fearless: watching you adapt to life on the Outside has given me hope and made me smile. Happy scratching!

To the Nack, always – it knows why.

To my Parents, for giving me everything I needed to achieve my ambitions, and more.

To all my In-Laws for their encouragement.

To my friends for asking politely.

To Ruth, for being the yardstick against which I will never measure up, and for being nice about it. You're the greatest.

And to Jim, for his faith and encouragement and for cutting me some slack when I needed it. Mentor and friend, I am profoundly grateful.

SECTION I

THE FOUNDATIONS

CHAPTER 1

INTRODUCTION

COMPUTER TERRORISM 'COMING TO BRITAIN' *The Independent, 28 November 1991*

AL-QAIDA PLANNING CYBER-ATTACKS *The Guardian, 28 June 2002*

CYBER TERRORISTS WHO COULD BRING BRITAIN TO A COMPLETE STANDSTILL *Sunday Express, 30 October 2005*

1. THE RESEARCH QUESTION

The ubiquitous presence of the Internet and the palpable sense that its pervasiveness leaves us vulnerable to threats from electronic wrongdoers is now firmly entrenched in Western societies, and cyberterrorism appears to be the latest incarnation of this threat. The Internet has become established at the heart of modern society relatively quickly. Its first incarnation was the ARPANET, established in 1969 by the US Department of Defense. It is often thought that the purpose of the original ARPANET was as a network architecture for the US military that could survive disruptions from the enemy, including a nuclear attack due to its distributed nature (Nader 1998). However, it has also been argued that ARPANET was, in reality, nothing more than a method of making the most economical use for research purposes out of what were, at the time, scarce computing resources (Raymond and Steele 1996).

Raymond gives an account of the genesis of the Internet as we know it today (Raymond and Steele 1996). It is likely that ARPANET's main function, as originally conceived, would have been to support early remote login and other forms of distributed computing. However, users soon realised the potential of early electronic mail technology and this came to dominate ARPANET's usage. This communication network steadily increased in importance as growing numbers of academics, researchers and many others, including hackers, started to connect. The next 25 years saw many changes, most notable among which were the development of computers to the stage where PC use was widespread in homes as well as in businesses; and the growing capabilities of the Internet's protocols, notably the shift from NCP/IP to TCP/IP in 1982

and the implementation of the Domain Name System in 1983. It was around this time that the collection of interconnected networks clustered around ARPANET came to be referred to as the "Internet".

In 1986, the National Science Foundation opened up access to five regional supercomputing centres through NSFnet, which became the backbone of the Internet. ARPANET formally closed down in 1990. NSFnet was then sold off to private telecommunications companies between 1990 and 1994 so that, ultimately, the Internet backbone became completely commercial. It was around 1994 that the Internet became mainstream as the public took to the hypertext and multimedia functions of the World Wide Web (Raymond and Steele 1996).

Growth in Internet users has been astonishing since then, with over 37.5 million users, representing over 60% of the population, in the UK alone as at September 2006 (www.internetworldstats.com/europa.htm). In December 2006, the use of high-speed broadband connections accounted for 79.2% of all UK Internet connections, up from 75.8% in September 2006 (National Statistics 2007). Turning to UK businesses, the value of Internet sales rose to £103.3bn in 2005, up 56% from 2004, while the proportion of businesses selling online rose by 22% over the same period. In 2005, nearly 75% of UK businesses reported using broadband, a rise of 25% on 2004; nearly 70% of UK businesses had a website in 2005, up by 4% on 2004; and the proportion of UK businesses using the Internet to interact with public authorities rose from 41% to over 50% between 2004 and 2005 (National Statistics 2006). At the national level, the UK government continues to integrate services into the electronic environment and has recently taken a step further in its acknowledgement of the importance of the electronic element of the critical national infrastructure by setting up the Centre for the Protection of National Infrastructure. This is an inter-departmental organisation which incorporates the work previously carried out by the NISCC, that is, the provision of advice and information on computer network defence and other information assurance issues, and integrates this information security advice with advice relating to personnel and physical security (www.cpni.gov.uk).

Headlines like those presented at the beginning of this Introduction will be familiar to anyone who reads a UK national newspaper on a regular basis. Having come to put so much reliance on the Internet and related technologies, the public has been made aware that everything from the critical national infrastructure (CNI) to their personal identities is threatened, most recently by cyberterrorists. Or is it? When an interested person digs

a little deeper, it turns out that most academics and many other experts agree that no terrorist organisation is so far known to have deliberately caused substantial damage by electronic means alone. This gives rise to several questions, not the least of which is how society got to the point of being concerned about a phenomenon which apparently does not yet exist.

My interest in this question arose out of research I did on hackers for a Masters degree in Criminology in 2000. This led to the insight that an understanding of the phenomenon of hacking and its consequences requires more than just the study of delinquent behaviour: it requires a broader understanding of technology in society to place that behaviour in context. A switch to the Information Systems (IS) discipline for doctoral research was indicated. It was whilst I was in the early stages of formulating my research question that the atrocities of 9/11 occurred. The horror I felt as I watched the towers of the World Trade Center collapse live on television affected me profoundly, as it did millions of others. As the story unfolded in the news over the weeks and months that followed, I listened to the stories of those who were killed and those who survived and admired the courage of a nation getting back to work, a nation which, unlike ours, was unused to terrorist attacks on home soil.

However, this admiration sat uneasily with another feature of the aftermath of 9/11, the call to arms and the hasty legislation enacted to 'address' the terrorist problem. Here were policies which were being rushed through with little meaningful debate using 9/11 as crude justification for very serious measures. In the UK, the Anti-Terrorism, Crime and Security Act 2001 was passed in a hurry and, despite a spirited opposition mounted in the House of Lords, contained contentious provisions including police access to personal records and retention of communications data. The problem was that these provisions applied to criminal investigations, yet were justified in Parliament with reference to arguments about terrorism. All of this was conducted against a background of media reports that al Qaeda operatives were using the Internet for planning and communication and that cyberterrorist attacks were imminent. The Internet was portrayed as somehow complicit with terrorism. As one journalist put it, "Can the internet do anything right? After a year of being blamed for the biggest speculative binge since the 1920s, it is now cast as the helpmate of modern terrorism" (*The Guardian*, 15 November 2001). No wonder the Government wanted enhanced access to communications data.

Here, then, was the opportunity for a study which encompassed my existing research interests of hacking, technology and society, but was made both timely and more intriguing with the addition of the elements of terrorism and the social control culture. Having observed what looked very much like Government policy-making and serious extensions of police powers based on the rhetoric of fear, I started considering the possibility that cyberterrorism looked rather like a moral panic. Certain groups, including the press and politicians, were making claims about the cyberterrorist threat, yet these claims appeared somewhat distorted. Most people I talked to seemed to know cyberterrorism was a problem but, when pressed, were not sure what it was or how prevalent it might be. Closer examination of numerous press reports revealed that many of the stories were familiar hacking tales dressed up as cyberterrorism. In short, high profile groups, the press and, in a rather woolly way, some members of the public seemed to be getting quite concerned about a phenomenon which did not yet seem to exist. Was the threat from cyberterrorism a social construction in the purest sense – a non-existent phenomenon which had effectively been brought into existence by public expressions of concern – and, if so, how had it been constructed, by whom and why? The task was, therefore, to deconstruct cyberterrorism.

2. RESEARCH APPROACH AND THE INFORMATION SYSTEMS DISCIPLINE

These were wide questions and a framework was needed in order to effect a scientific analysis of the social mechanisms at work. First, the three fundamental themes that run through this study – information and communication technology, hacking and terrorism – needed to be placed in their social context with particular attention to the socio-technical dynamic emphasised in the IS discipline. IS researchers have always addressed questions of technology and social change and have more recently considered the nature, use and impact of the Internet, together with policy aspects of the 'Information Society' (Avgerou 2000). By viewing cyberterrorism as a socio-technical artefact, it is located squarely within this tradition. Moreover, cyberterrorism is fundamentally a question of information security, a theme which has received extensive study within the IS field. A significant body of literature on cyberterrorism has been generated by information security researchers and this, along with literature from other fields, is reviewed in Chapter 2.

Chapter 3 introduces the concept of moral panic, which is borrowed from the reference discipline of Sociology (Keen 1980). It has its roots in a transactional approach to deviance, notable in its day for overturning the orthodoxy that deviance could be

identified and explained as a form of rule-breaking. Instead, deviance is seen as the product of a society which formulates rules and decides how to apply them. Deviance, on this view, is not a characteristic of the act itself, but a category constructed in the course of interaction between the 'deviant' and other powerful elements in society, notably agents of social control (Becker 1963). Moral panic has also been developed within the US in the constructivist tradition, which challenged the notion that social problems were self-evident. The task for sociologists was to expose and explain the social processes which define social problems and how those definitions are institutionally adopted and acted upon (Critcher 2003). Given that this study was based on a suspicion that cyberterrorism had more to do with social anxieties about technology and terrorism than with actual behaviour identified in terrorist cells, moral panic seemed an interesting way to approach the subject.

Chapter 4 outlines the interpretivist philosophies which underpin this study and how they tie in with a research method designed to untangle and make explicit the social processes which might have combined to construct cyberterrorism. Dhillon and Backhouse (2001) have noted that, in IS generally and information security research in particular, there has been a historical emphasis on the functionalist approach, with its associated notions of objective empirical reality and an essential integrated order in the social world. Such an approach fails to illuminate the interplay between technology and the social world and the complexity which derives from the indeterminate nature of human intention and behaviour. They argue for a greater focus on socio-organisational perspectives in IS and security research, based in the interpretative tradition, to allow exploration of the importance of concepts of power, authority, responsibility, influence and control (see also Galliers 1985; Galliers 1991; Lee 1991; Orlikowski and Baroudi 1991; Walsham 1995; Klein and Myers 1999; Mingers 2001; Mingers 2001a). It is hoped that the work recounted in this dissertation is another step along the path that they illuminate.

When a researcher sets forth to test out an idea, it is of paramount importance to demonstrate as rigorously as possible that all aspects of the phenomenon have been considered so that the conclusions drawn will have been amply demonstrated. This is particularly important with interpretative research, in which tradition the criteria for judging scientific research are less developed than in the positivist tradition. The IS domain has in the past been subject to criticism that the disparate nature of its themes and research approaches has led to a lack of scientific rigour (Avgerou 2000) and

strategies have been developed to address this criticism (for example, Galliers and Land 1987; Galliers 1991; Lee 1991; Orlikowski and Baroudi 1991; Klein and Myers 1999; Mingers 2001). Accordingly, a set of principles for enhancing scientific rigour are set out in Chapter 4 and were applied in the analysis and findings of this study, set out in Chapters 5-8. The findings are extensive because of the complexity encountered in the subject and the need to demonstrate a solid basis for the discussion and conclusions in Chapter 9, which reconsiders the questions about how cyberterrorism has been constructed, by whom, for what ends and whether it amounts to a moral panic. Finally, the contributions of this study and a number of avenues for future research are identified in Chapter 10.

CHAPTER 2

CYBERTERRORISM IN THE LITERATURE

1. OVERVIEW

There is a considerable, multi-disciplinary literature on cyberterrorism which has been growing steadily since the early 1990s and exploded following the atrocities of 11 September 2001. Around 60% of the total academic output originates in the period since 9/11, the events of that day having focussed the minds of many scholars on future terrorist strategies and how society might prepare itself. The number of terrorism courses offered by universities has also increased dramatically (Gordon 2005).

There are, roughly, three categories of contribution to a literature comprised of just under 300 articles. First, around 70% of the literature is security-oriented, most of it written by scholars of information security, computer science and military studies. This literature is almost exclusively written from within the positivist paradigm. The second category is political in nature and accounts for about 25% of the literature. It includes contributions from the disciplines of political science, international relations and law. The third category, representing the remaining 5%, includes many of the social sciences – sociology, psychology, anthropology, media studies – and considers the more human aspects of the socio-technical phenomenon of cyberterrorism.

The majority of commentators adopt the perspective of the United States. The US is a natural focus because it was the location of the most deadly terrorist atrocity of modern times; it is also technologically the most highly connected and dependent state in the world and, therefore, arguably the most vulnerable to cyberterrorist attack; and the US government has lavished more resources on research and infrastructure protection since 9/11 than any other nation (Giacomello 2004). The review below will often refer to the US position but the same or similar arguments may apply to the UK. Cyberterrorism is presented as a trans-national issue in the literature. There are important differences between the two countries, however. The experience of terrorist attacks on home soil is still a relatively new phenomenon for the US, whereas the UK has been living with the terrorist campaigns of the IRA, and al Qaeda more recently, for many decades.

Whereas the UK is more used to sustained nationalist terrorist campaigns aimed at economic and political harm, both countries are now coming to terms with a different type of religious fundamentalist terrorism, aimed more at mass casualties through suicide bombings, but the starting point for each nation's attempts at adaptation is necessarily different because of their diverse historical experiences.

A macro view of the literature reveals adherence to a risk analysis model, with contributions concentrating either on threats or vulnerabilities, sometimes both. Most studies concentrate on the standpoint of the potential victim of cyberterrorism, with the spotlight on vulnerabilities and reactions to 'what if' scenarios. This is understandable because analysis of the terrorist threat at first hand is problematic due to lack of access either to terrorist groups or to government intelligence which is classified. Those few attempts at structured analysis of the terrorist perspective are all the more important for portraying a sense, if only limited, of what the genuine level of the cyberterrorist threat might be.

There are several components necessary for an accurate assessment of the threat from cyberterrorism: a clear definition of cyberterrorism; a conception of who might engage in it; reliable information on how terrorists are currently using information communication technologies (ICTs); and a rigorous assessment of how likely it is that terrorists will progress from using technology in the normal course of their activities to attacks using computers. These factors will be assessed in turn below according to the existing literature.

The corresponding vulnerabilities also require detailed assessment and the identification of these is intimately bound up with views on the appropriate social reaction to the threat of cyberterrorism. The social reaction will, accordingly, be analysed at three levels: national, public-private relationship and international. First, it is necessary to determine a working definition of cyberterrorism.

2. DEFINITIONS OF CYBERTERRORISM

The military influence in the literature is apparent nowhere so much as in the debate over the definition of cyberterrorism. A number of terms have been coined which are frequently referred to and require some explanation.

2.1 Netwar

The concept of netwar was developed by Ronfeldt and Arquilla in the early 1990s to describe a mode of conflict at the societal end of the military-societal spectrum in which

small groups of actors can combine together using the new ICTs. Yet the emphasis of the concept is on organisation and doctrine rather than the technology (Arquilla and Ronfeldt 1999; Arquilla, Ronfeldt et al. 2000). It describes both conflict – especially non-military – and crime, and the actors are non-state, paramilitary, irregulars, criminals or activists. The organisational structure is flat, rather than hierarchical, with no central leadership and decision-making and operations are decentralised, guided by a shared set of ideas and interests. Attacks come in swarms, described as packeting. In terms of defence, the network structure itself is effective, since the destruction of parts of the network will not affect the viability of the whole.

This concept runs through much of the literature on terrorism and ICTs, even if it is not referred to by name. ICTs have made possible the emergence of a large number of networked organisations, terrorist, criminal, and activist, who can use their structures and technology to wield power at levels far greater than would otherwise be possible, achieving a degree of asymmetry. The traditional hierarchical structure of the state is seen as unwieldy and ineffective in combating networked organisations (Desouza 2005).

The trend within Middle Eastern terrorism is away from the traditional, state-sponsored, bureaucratic terrorist organisations of the 1960s and 1970s, towards the new-generation groups with more fluid and less hierarchical organisational forms which rely on a fundamentalist view of Islam for a radical ideology. Examples can be found in Hamas, Hezbollah, the Egyptian Islamic Group and al Qaeda. These groups are decentralised, with loose ties amongst dispersed units and individuals and decision-making tends to be delegated. Al Qaeda epitomises the notion of transnationalism, denoting international interactions between non-state actors. Although al Qaeda found assistance from state actors such as the Taliban rulers in Afghanistan, this is not the essence of the organisation, which has continued to operate long after the Taliban have been deposed. These new-generation terrorists rely on ICTs in order to maintain this structure and, increasingly, to coordinate activities and disseminate propaganda and ideology (Whine 1999; Zanini 1999; Whine 1999a; Arquilla, Ronfeldt et al. 2000). Zanini (1999) was prescient in noting the importance of the networked structure to the organisation now known as al Qaeda. She noted that:

> It is important to avoid equating the bin Laden network solely with bin Laden. He represents a key node in the Arab Afghan terror network, but there should be no illusions about the likely effect on the network of actions taken to neutralize him. The network conducts many operations without his involvement, leadership or financing – and will continue to be able to do so should he be killed or captured.

2.2 Information warfare

If netwar is predominantly about organisation and doctrine, then information warfare (IW) is about offensive and defensive control of the information environment. There is fierce debate about the definition of IW, with those at one extreme claiming that future wars can be won with information dominance and without bloodshed and sceptics at the other extreme claiming that information control has always been key in warfare (Rathmell 1997). Schwartau (2000) takes a very broad view of IW, including intimidation of individuals, corporate espionage and inter-state conflict. He underlines the current state of asymmetry, in which conventional US military forces are overwhelmingly more powerful than their enemies. Unable to fight the US on its own terms, Schwartau foresees smaller opponents seeking asymmetries of their own: engaging in terrorist activities which lie outside internationally accepted modes of behaviour against an enemy constrained by democratic principles; and seeking out IW as a means of fighting a more powerful enemy which represents a much larger, more IT dependent and, therefore, more vulnerable target. As this example demonstrates, asymmetries can be characterised as positive and negative, with the former generating an offensive advantage and the latter a vulnerability (Kshetri 2005a). Schwartau warns that the US fails to take IW seriously at its peril, claiming that "asymmetrical conflict is now the norm ... [and] is the only strategy that makes sense for erstwhile allies as well as enemies, since they cannot compete under traditional rules". The fact that it makes sense does not, of course, mean that the threat is as imminent or as great as Schwartau claims.

More moderate definitions of IW include "targeting the information and information systems that comprise and support civilian and military infrastructures of an adversary" (Devost, Houghton et al. 1997); and "activities carried out ... with specific political and strategic objectives, aimed at the integrity, availability and confidentiality of the data collected, stored and transferred inside information systems connected to the Internet" (Valeri and Knights 2000). However, the important element is that IW constitutes attacks on information activities generally, not information systems specifically (Rathmell 1997).

The centrality of information control in the military environment has been termed a Revolution in Military Affairs, so that "The fight to obtain an information advantage will take place in the physical space with bombs and bullets, in the cyberspace with hackers and jammers, and in the "mental space" with deception and psychological

operations" (Brown 1996). Data are operational targets and a tactical goal of IW is to manipulate this data and transform it into information to further a political or strategic objective so that, for example, the enemy is induced to act on false information (Valeri and Knights 2000). Thus, IW is about more than just electronic operations, it concerns the information itself.

Netwar and IW are not synonymous, but do converge in networked groups using ICTs to engage in IW (Zanini 1999). On the other hand, IW can also be waged by state actors from within the normal hierarchical paradigms. The US military, for example, reportedly used viruses and hacking techniques against Iraqi air defences in the first Gulf war and engaged in cyber-disinformation campaigns, gathered intelligence and distorted data received by Serb gunners in the conflict in the former Yugoslavia (Arquilla 2000; Stanton 2002). Such mechanisms can be seen as both offensive and defensive, at the same time compromising the ability of the enemy to use its information systems effectively and protecting against electronic and physical counterattack.

2.3 Cyberterrorism

Cyberterrorism, also referred to in the literature as 'information terrorism', is a subset of both information warfare (Devost, Houghton et al. 1997; Rathmell 1997; Schwartau 2000) and terrorism and can be considered as the area of overlap between terrorism and information warfare. Defining cyberterrorism is problematic, however, for several reasons. First, the term is often used broadly and without rigour, particularly in the news media (Post, Ruby et al. 2000; Embar-Seddon 2002; Gordon and Ford 2002; Weimann 2005). There is confusion between cyberterrorism and cybercrime, terrorists and hackers coupled with a failure to distinguish between terrorist use of ICTs as a facilitator of activities and use of ICTs as either weapon or target (Ingles-Le Nobel 1999; Conway 2002; Weimann 2005). Second, there is a tendency to create neologisms by placing cyber-, computer- and information- in front of other words to create seemingly new concepts which are, in reality, rarely new at all (Embar-Seddon 2002; Weimann 2005). Third, there is no settled definition of terrorism itself (Rabbie 1991; Reid 1997; Ballard, Hornik et al. 2002; Embar-Seddon 2002). Terrorism is usually defined as including an element of actual or threatened violence aimed at communicating a message to or influencing a target audience wider than the immediate victims in an attempt to achieve political objectives (Rabbie 1991; Reid 1997; Richardson 1999). The terrorism literature is heavily influenced by governments, particularly the US government who, through preconceived policies and programmes,

have had an impact on definitions of terrorism, the types of data used, selection of research problems, dissemination of findings and marketing of ideas. Yet, even within one government administration, different departments may work to different definitions of terrorism (Mahmood 2001) highlighting the fact that its definition is a politically vexed question, often having as much to do with vested interests as anything else. This has lead some researchers to adopt a classification-based approach rather than wrestle with one all-encompassing definition (Ballard, Hornik et al. 2002).

The lines of debate on the definition of cyberterrorism can be drawn in a number of different ways. There is the division between those who require violence or the threat of violence as an element of the definition (Pollitt 1998; Conway 2002a; Iqbal 2004) and those who do not. The latter group is far more numerous. Alternatively, Ballard, Hornik et al. (2002) discern three broad patterns in attempts to define cyberterrorism. The first group use one of the existing definitions of terrorism, altered to account for the electronic element. Barry Collin at the Institute for Security and Intelligence in California coined the term 'cyberterrorism' in the 1980s to refer to the convergence of cyberspace and terrorism (Denning 2000). Cyberterrorism has been defined as "premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub national groups or clandestine agents" (Pollitt 1998; Conway 2002a); "politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage" (Denning 2000); and "an individual who uses computer/network technology to control, dominate or coerce through the use of terror in furtherance of political or social objectives." (Rogers 2003).

There are others in this first group who espouse very wide definitions of cyberterrorism, setting aside the requirements of violence, serious harm and terror and claiming that all terrorist use of computers is cyberterrorism, not just their use as tools or targets (Desouza and Hensgen 2003). Foltz (2004) achieved a similarly broad definition by amalgamating many of the major definitions which had come before:

> ... cyberterrorism is an attack or threat of an attack (Denning 2000a), politically motivated (Denning 2000a), intended to:
>
> - Interfere with the political, social (Denning 2000a), or economic (McFeatters 2001) functioning of a group, organization, or country; or
> - Induce either physical violence (Pollitt 1998) or the unjust use of power; or
> - In conjunction with a more traditional terrorist action (Bronskill 2001).

Such broad approaches strip the term of all sense, including under the umbrella of cyberterrorism much that would commonly be regarded as criminal and rendering it a blunt tool for any meaningful discussion about either the cyberterrorist threat or counter-terrorism policy.

Second, there are definitions which are predicated on existing legal definitions, so that reference is made to unlawful attacks against information systems to intimidate or coerce to promote political or social objectives (Denning 2000a). The definitions of terrorism and cyberterrorism may not have settled in the political literature, but the law provides an authoritative, although not incontrovertible, definition (Walker 2000). In the UK, the Terrorism Act 2000, Section 1(1) defines terrorism as an action or threat of action which is designed to influence the government or intimidate the public for a political, religious or ideological cause. Section 1(2) sets out the types of action which constitute terrorism, which include violence against the person, but also serious property damage and endangering life, health or safety of individuals. Cyberterrorism is expressly provided for in section 1(2)(e), defined as action designed seriously to interfere with or seriously to disrupt an electronic system. Section 1(4) gives the definition extra-territorial application. Crucially, this definition of cyberterrorism dispenses with the need for violence or even damage to property, since interference or disruption of an electronic system does not necessarily imply either.

Third, there are attempts to combine definitions of terrorism with a classificatory approach. Gordon and Ford (2002) attempt a reductionist approach, splitting definitions of terrorism into their component parts and analysing the impact of ICTs on each element. This results in a wide definition of cyberterrorism, encompassing all forms of terrorist use of ICTs. They argue that a narrow definition of cyberterrorism leads to undue compartmentalisation of approaches to solutions, whereas the 'cyber' element of terrorism should be accounted for in all areas of the counter-terrorism model. This is quite true, but the same effect can be achieved by recognising terrorist uses of ICTs as points on a continuum, with cyberterrorism at the extreme end. Such an approach requires a narrow definition of cyberterrorism but, at the same time, recognises the need for solutions to all other points on the scale. An over-wide definition of cyberterrorism, on the other hand, can lead to disproportionate counter-terrorist measures which are not effective in countering the perceived threat and risk impinging on civilian liberties.

Using similar arguments to Gordon and Ford, Desouza and Hensgen (Desouza and Hensgen 2003; Hensgen, Desouza et al. 2003; Desouza and Hensgen 2003a) outline a

semiotic approach to the study and prediction of cyberterrorism. On the first, morphological rung of the semiotic ladder, the task is to assess the ICT-related activities of individual terrorist agents. At the next, empirical level, the task is to group like with like based on characteristics identified at the morphological level, finding, for example, patterns of behaviour which may point to communication between members of a terrorist cell. The syntactical level focuses on identifying and defining patterns and relationships between agents and objects observed at the morphological and empirical levels. The semantic phase then places these patterns and relationships in a systemic context. Terrorist attacks at this level focus on destruction or large-scale disruption of the critical national infrastructure (CNI) and the attacker would require both technical skills and systemic knowledge in order to exploit weaknesses. Desouza and Hensgen consider that most of the cyberterrorism literature is focussed at this level. Finally, the response to what has been learned at previous levels is formed at the pragmatic level. Moreover, it is not possible to prevent attacks higher up the semiotic ladder without first dealing with issues arising at the morphological and empirical levels. This semiotic framework appears instructive until the authors claim that the distinction between cybercrime and cyberterrorism should be eliminated since it is merely a semantic distinction: both involve the intent to destroy. This contention is false. Terrorist intent goes beyond criminal intent in its aim of terrorising an audience beyond the immediate victim for political advantage. This is where their model breaks down and the fault lies in their over-wide definition of cyberterrorism. There must also be a line between terrorist use of ICTs and cyberterrorism (see further section 4) because of the consequences at the pragmatic level – retributive social consequences – of defining behaviour on the lowest rungs of the semiotic ladder as terrorist.

Devost, Houghton et al. (1997) also take a classificatory approach and adopt a wide definition of cyberterrorism as "the intentional abuse of a digital information system, network or component toward and end that supports or facilitates a terrorist campaign or action". This definition is wide in that 'cyberterrorism' does not require violence and need only support or facilitate a terrorist campaign, a position which seems to include disruption as well as destruction. Much of the literature on cyberterrorism adopts, implicitly or explicitly, the second part of the analysis of Devost, Houghton et al., which comprises a matrix-based classification of terrorist acts, setting physical/digital targets against physical/digital tools.

		Target	
		Physical	*Digital*
Tool	*Physical*	**(a)**	**(b)**
	Digital	**(c)**	**(d)**

Source: adapted from Devost, Houghton et al. (1997)

It is important to notice that the definition of terrorism must be applied first, only then does the matrix classification operate. Cell (a) represents conventional terrorism. According to the authors, the other three categories are cyberterrorism and cell (d) is said to be 'pure' cyberterrorism. Cell (b) represents a conventional attack on a high-tech target and the authors give the example of IRA bombings in the City of London. I cannot agree that this is 'cyberterrorism', since any damage to information systems in such an attack is usually considered collateral damage. The same effect occurred with the atrocities of 9/11: some trading activity was disrupted in the following days due to the geographic concentration of the financial services industry and its dependence on the badly damaged communications infrastructure (Marlin 2001), yet 9/11 has never seriously been labelled a 'cyberterrorist attack'. This was collateral damage. Accordingly, type (b) incidents are treated as conventional terrorism in this study.

Cell (c) is more ambiguous. Devost et al. give the example of an electronic attack on an air traffic control system intended to cause a plane crash. This might more naturally be labelled cyberterrorism. Indeed, many of the disaster scenarios commonly presented, such as electronic attacks causing train crashes, bursting dams, nuclear reactor explosions, are of this type (Shockwavewriter 2000). The President's Commission on Critical Infrastructure Protection (PCCIP 1997) foresaw grave danger from cyberterrorists who might cause explosions in power stations through virus attacks on the computer command centre or render pharmaceuticals lethal by accessing the processing control system of a drug manufacturer to alter the formulae. The element of terror is strongest in cell (c), although there are bigger questions about whether such attacks are possible or likely (Pollitt 1998).

This contrasts with cell (d), which undoubtedly represents cyberterrorism in its pure form, if only one can argue that the element of terror is present. In an earlier version of this paper (Devost, Houghton et al. 1996), the authors argue that terrorism scholars who view physical violence as a necessary component of terrorism should broaden that view

to reflect the centrality of technology in modern society. However, this argument only works once the attack has reached a certain level of seriousness. A virus or denial of service (DoS) attack, if perpetrated by a terrorist group, arguably does not amount to cyberterrorism because the result tends to be disruption, rather than destruction and fear. On the other hand, a successful electronic attack by terrorists on the London Stock Exchange, bringing trading to a halt for a significant period of time, might be regarded as sufficiently serious to qualify as a cyberterrorist attack, leaving aside the question of whether such an outcome is possible in these days of distributed computing. The PCCIP certainly defined as cyberterrorism the disruption of banks, international finance transactions and stock exchanges leading to a public loss of trust in the economic system (PCCIP 1997). Nevertheless, an attack would have to be on an unprecedented scale in order to achieve such an effect.

Post, Ruby et al. (2000) take a somewhat different approach, using a three-part test to determine whether a particular attack amounts to cyberterrorism. The attack should be:

1. ideologically motivated;
2. use and/or target an information system by either digital or physical means to affect the information system itself or persons or property dependent on it;
3. intended to influence, intimidate or coerce an audience beyond the immediate target of the attack.

Limb 2 of this test embodies the same matrix approach as Devost, Houghton et al. and includes in the definition a physical attack on an information system (cell b), a position which is not accepted in this study. However, limb 3 of the test renders this definition narrower than that used by Devost, Houghton et al. because it looks behind the attack to the intentions of the perpetrators and beyond the attack to its effect on the ultimate audience. On this analysis, however, hacktivism – using hacking techniques against an electronic target with the intent of disrupting normal operations but not causing serious damage (Denning 2000) – by political activist groups who would not usually be thought of as terrorists would also qualify as 'cyberterrorism'. Post, Ruby et al. suggest that hacktivism and cyberterrorism exist at different points on a sliding scale and that the difference between the two is likely to reduce to "a qualitative analysis of the degree to which the attack was designed to produce fear and intimidation in a target audience in order to accomplish an ideological goal".

2.4 Definition of cyberterrorism adopted in this study

The following definition blends a number of the approaches outlined above. Cyberterrorism is:

1. an action or threat of action which is designed to engender fear or terror so as to influence the government or intimidate the public for a political, religious or ideological cause; and
2. the action involves use of digital means to attack a digital target, the direct consequences of which may be tangible or intangible and which are sufficiently serious as to be likely to cause the effects in part 1.

This definition does not focus on the nature of the damage. This circumvents the arguments about the type of damage necessary to qualify as terrorism: does violent injury, damage to property, economic damage or minor disruption constitute terrorism? Such arguments become difficult when the target is digital. Rather this definition focuses on the psychological effects on a wider population, the essence of terrorism. Any type of damage will qualify and the only question is whether it is likely or not to engender fear or terror. On this model, an attack causing widespread economic damage may be sufficient if it causes such economic instability that people fear for their financial wellbeing. Fear of losing the economic means to a good life may be equally coercive as the fear of physical violence. On the other hand, an attack causing an outage of some part of the CNI will not qualify unless its severity is on an unprecedented scale. People routinely suffer interruptions in electricity, telephone and water services, sometimes for days at a time, and there is rarely any sense of fear or panic. Cyberterrorism goes beyond fear and terror, however, because it requires the perpetrator to be acting in furtherance of a cause, political, religious or ideological. Thus, a group mounting a major attack for personal gain are not terrorists even though they may cause fear and terror.

The matrix of Devost, Houghton et al. (1997) is integrated into the definition above, but with modifications. Only use of digital means qualifies as cyberterrorism. A bomb exploding the physical components of a network would not count: this is conventional terrorism. Further, cell (c) (digital tool/physical target) is misleading, because any digital attack aimed ultimately at a physical target requires interference with an electronic system which *in turn* causes damage to a physical target. Thus, cells (c) and (d) are both digital attacks on digital targets but, in cell (c), the ultimate aim is that the compromised digital target will result in *tangible*, catastrophic, physical consequences,

whereas, in cell (d) the ultimate aim is to cause catastrophic, *intangible* consequences, such as commercial meltdown and huge economic losses. With this clarification, the distinctions made by Devost, Houghton et al. are retained in the definition used in this study.

This definition of cyberterrorism is deliberately restrictive. It draws a clear distinction between cyberterrorism and cybercrime. Both fit into the matrix part of the definition, and this will be explored in chapter 4, but only cyberterrorism fulfils the first limb of the test. It also draws a clear distinction between terrorist use of ICTs and cyberterrorism, since the former does not of itself inspire fear or terror.

3. WHO ARE THE CYBERTERRORISTS?

Social awareness of cyberterrorism is high due to a combination of psychological, political and economic factors (Weimann 2005). Both terrorism and technology are established sources of social anxiety capable of inspiring public fear and concern (Sandywell 2006). The combination of the two results in potent anxiety. The mass media have been assiduous in their pursuit of alarmist headlines about what terrorists, particularly al Qaeda, are capable of. Likewise, there have been many films and novels which have exploited the dramatic potential of cyberterrorism. If terrorism and technology inspire fear, it is partly because they are also sources of ignorance. The public do not understand the issues but then, arguably, nor do policy makers and those who influence them. As a result, hackers are confounded with terrorists and terrorist use of ICTs is characterised as cyberterrorism. Such confusion of distinct issues is not helpful since there is no coherent target at which to aim counter-terrorism policy.

There is a pressing need to distinguish between all the possible sources of an electronic attack (Vatis 2001; Schell and Dodge 2002) and acknowledge that, so far, no publicly documented attack has ever been made by a terrorist group (Denning 2000a; Weimann 2005), although this does not preclude the possibility that such an attack has taken place but that this information has not been released into the public domain. Hackers, on the other hand, are known to be active and much of the myth surrounding cyberterrorists can be understood by looking at the long and chequered history of hackers in the public psyche. There is a paucity of empirical research on hackers and most literature relies on conjecture, hearsay and myth (Schell and Dodge 2002). Skibell (2002) has written that hackers as a conceptual, as opposed to real, group obtained cohesion with the attribution of certain characteristics unique to them. A distinct psychological discourse emerged which attributed to hackers a pathological addiction to computers, locking themselves

away from the real world and engaging with others solely through the clinical interface of a computer. A second set of attributed characteristics emerged, in which hackers had almost magical, unlimited powers to break into systems, a theme which subsists today in the myth of the cyberterrorist capable of causing death and destruction by hacking into the CNI. With the increasing computerisation of society, hacking was perceived as an escalating threat and was re-characterised from nuisance to crime, with hackers becoming all-powerful, underground criminals. Hackers may even have been complicit in their own demonisation. If hackers publicly expose security flaws and many are happy to boast about it, often enhancing accounts of their own prowess in the process, they are seen as threatening, mysterious, powerful and dangerous. There is also an element of shooting the messenger in public hostility towards hackers (Weimann 2005). The myth of hackers as a cohesive and coordinated social group with a dangerous agenda became entrenched as fact and no distinction between different types of attacker was recognised.

The next stage of the hacker myth is now evolving towards terrorism (Halbert 1997). Whereas previously the hacker was seen as an adolescent challenger to the adult order, bent on destabilising adult-created computer-dependent systems, now the cyberterrorist is seen as challenging the computer-dependent systems on which nations' infrastructures are founded. Just as Skibell found that, contrary to popular perceptions, most computer hackers are neither dangerous nor highly skilled, so too with cyberterrorism.

There is one category of actor which, many agree, is far more dangerous than all others: the insider (Brull and Wagley 2001; Hinde 2001; Weimann 2005). Even this common perception may be false, as the CSI/FBI survey has consistently found that the numbers of attacks coming from the outside are roughly the same as the numbers from the inside year on year (CSI/FBI 2005). This says nothing about seriousness of damage resulting, however. An insider is more likely than others to have sufficient information on the layout of a critical system and sufficient access to perpetrate a successful electronic attack on a critical system. There is a long history of attacks perpetrated by disgruntled employees and there is a genuinely merited fear that the best and most certain method for a cyberterrorist would be to infiltrate the target organisation. Whether the resulting damage would be as extensive as the scaremongers have claimed is debatable. A 2004 survey found that the most serious incidents were roughly equally caused externally and internally (PWC/DTI 2004).

One of the key problems for those trying to crystallise the issues is that cyber-attackers can relatively easily achieve anonymity, so that it can be very difficult for victims to trace the source of an attack (Jones 2005). Hackers, insiders and cyberterrorists are, therefore, easily confounded because it is almost impossible to establish definitively which it was. This suits those with an interest in amplifying the problem. For example, media reports overwhelmingly fail to distinguish hackers from terrorists, with escalated accounts making better stories. Concerns have been raised about the motivations of politicians in promoting anxiety about cyberterrorism, with insinuations of ulterior motives (Hosein and Whitley 2002; Weimann 2005), for instance justification for extending the national security apparatus (Halbert 1997) or for aggressive stances towards suspect nations like Iraq (Weimann 2005). If ignorance can be exploited for ideological reasons, it can also be exploited for commercial ones and it is certainly true that the IT security industry has done very well out of governments and organisations concerned about the threats from cyberterrorism.

4. TERRORIST EXPLOITATION OF ICTS

Terrorism is evolving in tandem with new uses of ICTs which broaden the spectrum of conflict and foster networked organisations (Whine 1999). Most commentators agree that modern terrorist groups currently make plentiful use of ICTs in the everyday running of their organisations (Ingles-Le Nobel 1999; Gilmore Commission 2002; Newton 2002; Stanton 2002). Some even argue that ICTs have facilitated the creation of and shaped modern terrorist and activist groups (Crilley 2001).

Whine (1999) notes the many benefits of ICTs to terrorist organisations (also Goodman, Kirk et al. 2006): they allow communication and networking, both internal and external to the group; secrecy and anonymity, both amongst themselves and from the outside world; low financial cost; a force multiplication effect, effectively allowing David to fight Goliath whilst at the same time remaining well-defended; and target audiences are within easy reach for the spreading of propaganda, particularly when traditional media channels are closed to extremists. The single effort of developing one exploit is sufficient to unleash multiple, synchronised attacks (Desmedt 2002). All of these factors are supportive of netwar. Danitz and Strobel (1999) have also highlighted as advantages the low cost of Internet communication; organisational advantages, particularly in mobilising large numbers of geographically diverse individuals; fast access to up-to-date information and intelligence; and replication and rapid dissemination of successful strategies.

As disadvantages, Danitz and Strobel note that Internet communications can easily be monitored and intercepted; opponents can sabotage Internet activities; information disseminated via the Internet can be inaccurate; the digital divide – the ICT 'haves' and 'have nots' – can be problematic, particularly for non-English-speaking groups; and decentralised, networked organisations relying on ICTs for communication may become unstable more rapidly than centralised, hierarchical organisations. Certainly, the US has noted that modern terrorist organisations' reliance on ICTs creates an opportunity for their counter-terrorist forces to gather intelligence and compromise operations (Gilmore Commission 2002).

Conway (2002) distinguishes four points on a spectrum of uses of the Internet for political activism, ranging from terrorist 'use' of the Internet at one end, through 'misuse' and 'offensive use', to 'cyberterrorism' at the other. Terrorist activities, she finds, have hitherto focussed on the first three tiers, with the vast majority of activity amounting only to terrorist 'use' of the Internet. Such use is a necessary and inevitable part of netwar and does not of itself amount to cyberterrorism, which she defines narrowly. Terrorist 'use' of the Internet amounts to online activity which would be perfectly legal if done by an ordinary member of the public, such as association, communication, intelligence gathering through legitimate searches and dissemination of information and messages about an organisation. When done by terrorists, this last is usually considered propaganda and studies have revealed that spreading propaganda via the Internet is quite persuasive, especially when the receiver is either neutral or sympathetic to the cause (Lee and Leets 2002). Moreover, use of the Internet by extremists is not a new phenomenon, the use of bulletin board systems being well documented in the early 1980s. Modern terrorist organisations such as Hamas and Hizbollah have dedicated websites and, although al Qaeda is an exception in this respect, its use of the Internet for email communication and research into potential methods of physical attack is documented (Levin 2002). Whilst some websites may just contain information about a given terrorist organisation, others have crossed the boundary from 'use' into 'misuse' or 'offensive use' by inciting violence against or murder of Westerners, particularly Americans and there have been discussions about what legal recourse authorities may have to prevent this (Crocco 2004; Hawkins 2005).

Denning (2000) has noted the widespread, non-disruptive use of the Internet by terrorists in support of their cause and has also commented on misuse and offensive use of ICTs. She characterises these as 'hacktivism' – using hacking techniques against an

electronic target with the intent of disrupting normal operations but not causing serious damage – but the perpetrators are usually groups or individuals other than terrorists. There are limited examples of terrorists engaging in hacktivism. They may, however, support their activities financially through both legitimate Internet-based businesses and Internet-facilitated fraud (Valeri and Knights 2000). The latter would fall into Conway's 'misuse' category. The most frequently cited example of offensive use is that of the Tamil Tigers, who swamped Sri Lankan embassies with 800 emails a day for two weeks, thereby generating publicity for their cause. There are no verified virus or worm attacks perpetrated by terrorists, but Denning notes that this is potentially a potent tool in their hands. There is also the prospect of semantic attacks, in which attackers surreptitiously alter the meaning of text on information-based sites such as news websites in order to convey false information or messages (Jones 2002).

Rathmell (1997) categorises use of IW by sub-state groups, notably terrorists but also including criminals and individuals, into:

1. new techniques applied to traditional activities, including intelligence gathering, communications, finance and propaganda;
2. old techniques applied to new activities, involving physical attacks against information activities including information infrastructures;
3. new techniques applied to new activities, being digital attacks against information activities.

This scheme constitutes an amalgamation of the matrix definition of cyberterrorism provided by Devost, Houghton et al. (1997) and Conway's (2002) sliding scale of terrorist use of the Internet. Consistent with other scholars, Rathmell finds that terrorists are active in category 1, have occasionally attempted category 2 attacks, but are not yet active in category 3.

5. THE RISKS FROM CYBERTERRORISM

There is not yet an academic consensus on the risks from cyberterrorism. Desouza and Hensgen (2003) note two schools of thought. The first holds that cyberterrorism is a myth, recalling the Millennium Bug which was ultimately easily correctable and did not produce the disasters predicted (Desmedt 2002). The second, mostly comprising technical specialists, contends that the threat is real and points to huge economic losses already caused by cyber-attacks.

Due to a lack of hard evidence, the literature tends to focus on modelling vulnerabilities and/or threats. On the vulnerability side, it is almost trite that any analysis commences with a picture of a society increasingly reliant on IT and correspondingly vulnerable to increasing information security threats. Although formal use of scientific risk assessment principles has been mooted in connection with terrorism (Anderson 2002; Deisler 2002; Garrick 2002; Haimes and Longstaff 2002), to the extent that vulnerability studies of the CNI have been carried out, they are largely classified and the results not openly available (Garrick 2002). The Internet is a particular concern since there is a duality in the vulnerabilities it creates. On the one hand it is the conduit by which attacks *might* be carried out against the CNI and other targets; on the other hand it appears to be a target in its own right as a vital infrastructure (Walden 2005). Yet, although the Internet itself may appear to present an obvious target for terrorists (Brunskill 2002), using the Internet may be more important to terrorists than its destruction.

In a careful analysis of the issues of critical infrastructure protection, Rathmell (1999) identifies a number of reasons for society's increasing vulnerability, including the rapid adoption of open-network architectures and the fact that a combination of privatisation, deregulation and globalisation of key industries has removed the owners and operators of important, trans-national networks from government control. Devost and Houghton (1996) predict that, as the military-industrial complex becomes increasingly dependent on technology, so it is increasingly likely that this technology will become a focus for attack. In addition, 9/11 has amply demonstrated that geographic boundaries are no longer a good defence against enemies, and the potential for electronic attack compounds the problem (PCCIP 1997; Wehde 1998).

On the threat side, the positive reasons for turning to cyberterrorism from a terrorist perspective have been set out: low cost, anonymity, variety and number of targets, remoteness and asymmetric characteristics of attack (Weimann 2005). Threats are thought to have increased, at the lower level of seriousness because of increasing IT literacy and ready access to tools for low-level attacks and, at the higher level, because nation states are pursuing the strategic military development of IW and information operations (IO) (Rathmell 1999). A change of terrorist strategy towards increasing attacks on vulnerable information structures may be imminent (Arquilla, Ronfeldt et al. 2000; Bunker 2000; Crilley 2001). Embar-Seddon (2002) has claimed that there are currently terrorists with hacking skills who are most likely to use those skills for force

multiplication. This would work at three levels: first, web propaganda might achieve the illusion that a terrorist group is bigger and more powerful than it is; second, literal force multiplication might be achieved with the recruitment of new members via the Internet; third, technology might be used as a force multiplier to magnify the harm caused during a conventional attack, disabling emergency communications, for example. Embar-Seddon does not quite arrive at the concept of asymmetry described above, but that would form a logical part of this third level.

Post, Ruby et al. (2000) reason that capability alone is not a sufficient measure of risk because it tends towards overestimation. Intention and context are, therefore, essential in risk evaluations for cyberterrorism and they list several factors indicating increased risk, including: the terrorist group identifies computers and networks as tools used by an adversary for security or dominance; the group leader is computer literate or growing computer literacy of group members; information-rich and -dependent environments post-industrial societies; offensive use of computers against a terrorist group; and successful offensive information operations of a rival terrorists group. Post, Ruby et al. also highlight the influence of what they call virtual group dynamics, in which communities of belief develop in online associations, characterised by high conflict, low cohesion, limited stability and strong resistance to hierarchical forms of leadership and control. They see this as fertile ground for terrorist groups, both in terms of their general operations and the possibility that disaffected, skilled hackers may be drawn into such organisations through online contact, then use their skills for terrorist purposes. They see the future threat of cyberterrorism coming from a subset of alienated individuals from within the hacker culture who are seduced into pursuing an anti-authoritarian agenda from within social-revolutionary terrorist groups. Denning (2000a) finds this unlikely, asserting that hackers mostly lack the motivation, organisation and psychology for violent attack or severe social or economic harm (also Embar-Seddon 2002; Schell and Dodge 2002). Post, Ruby et al. conclude, however, that there are four main reasons why a major cyberterrorist attack has not yet occurred: attacks targeted against the CNI or calculated to cause human casualties are extremely difficult to achieve; conventional means of attack remain the most effective; terrorists are not inclined to threaten an information structure on which they themselves rely; finally, the range of hacker targets has traditionally been narrow, confined mostly to ideological opposition to use of the Internet by government and corporate interests.

Given the lack of concrete evidence of terrorist intentions, scholars have attempted to model terrorist behaviour as a means of gauging the threat. Rabbie has mapped a behavioural interaction model which offers a social-psychological framework for examining terrorist behaviour over time (Rabbie 1991). The model effectively links together a number of different theories of behaviour, each of which operates at a different level and the last of which is interesting for present purposes. Rabbie cites the theory of reasoned action in which it is assumed that, where there are competing tendencies towards specific actions, the actor will choose that action which (1) appears to achieve his goal, (2) has a high probability of success, and (3) results in the most favourable cost/benefit analysis. These factors are instrumental in the formation of intention which is, in turn, the best predictor of behaviour.

Applying this part of Rabbie's model to cyberterrorism, the terrorists concerned would have to believe that their goals would be achieved by a cyber attack, that the attack has a high probability of success and that the cost/benefit analysis would lean in favour of the attack. Only then might an intention to commit cyberterrorism be formed which, in turn, would be a good indication that it might actually happen. When put like this, problems arise for those who claim that cyberterrorist attacks are imminent. First, it is doubtful whether a cyber attack is capable of inspiring fear in its victims and others, rather than annoyance or exasperation. As one industry insider put it:

> At the moment, the only way that you will scare most people with 'cyber' capabilities is to threaten to throw the equipment at them. (Jones 2005)

The goal of terrorising a section of society might not easily be achieved through cyberterrorism. Second, only a handful of hackers are capable of executing targeted attacks producing very specific outcomes and, even then, many critical systems have failsafes (Pollitt 1998). The probability of success may, in fact, be quite low, especially when compared with highly successful conventional terror campaigns. Third, despite many claims about the positive benefits for terrorists of adopting cyberterrorism, the cost/benefit analysis may not actually indicate this. Giacomello (2004) has conducted a careful cost-benefit analysis of cyberterrorism from a terrorist point of view and concluded that it was not an efficient substitute for traditional tools such as bombs and that online propaganda and activism were more effective ways of exploiting electronic media.

Present conditions being what they are, Rabbie's model suggests that terrorists are unlikely to form an intention to perpetrate a pure cyberterrorist attack and, intention

being the best predictor of behaviour, are unlikely to carry it out. This does not preclude the possibility of a cyber attack ancillary to a conventional attack, however, nor does it say anything about future conditions. Assuming a terrorist group actually attempted a cyber attack now or in the future, the outcome of that attack, successful or not, would feed back into the future decision-making process, according to Rabbie's model. Put another way, if pure cyberterrorism is as hard to achieve as many commentators suggest, terrorist groups might well abandon further attempts for the foreseeable future.

Giacomello's formal cost-benefit analysis (2004) also characterised terrorists as rational choice actors and bears closer scrutiny. He concluded that the technological environment is not yet sufficiently advanced, meaning that societies are not sufficiently IT dependent and terrorists do not have ready access to the requisite skills, for cyberterrorism to be attractive as a mainstream mode of attack. Even if attacks on the CNI could theoretically produce the kind of devastation terrorists seek, the expertise required for such an operation is currently so rare that terrorist groups would almost certainly have to hire mercenaries and the evidence is that most are extremely reluctant to do this, especially when conventional terrorism is still relatively cheaper, easier, more certain and can be achieved 'in-house'. The only entities with sufficient resources to launch an effective information attack against a nation state are other nations, and only wealthy ones at that. The gravest damage would likely be to the economy, both national and global, and to trust in information networks. This may act as a disincentive for foreign nations as they would be directly or indirectly affected by the damage. A central pillar of Giacomello's thesis rests on his finding that there is no conclusive evidence that physical destruction can result from an electronic attack on the CNI, leading him to conclude that, for the foreseeable future, terrorists are only likely to use electronic tools to leverage a wider, conventional attack.

A different view is provided by Devost, Houghton et al. (1996) who have applied a similar, 'reasoned action' model to cyberterrorism. They claim that terrorists will increasingly adopt technologically oriented tactics and strategies as technology becomes more cost-effective to them: financial and other costs diminish whilst availability and potential scale of disruption increase. The likelihood of success is increased by targeting modest goals to ensure success and visibility (Hoffman 1994), leading to low-risk, high-visibility outcomes. Devost, Houghton et al do not explain, however, how attacks on more modest goals will lead to terror, as opposed to mere disruption. In

addition, low-level attacks on information systems are often difficult to identify, since it is surprisingly difficult to establish whether a complex system is actually in good order (Brunskill 2002). Attacks which either go unnoticed or are discovered only much later are likely of little interest to terrorists pursuing a high-visibility goal (Lewis 2002).

Cilluffo and Gergely (1997) note the increasing use of technology by terrorist groups in the execution of their objectives, gathering intelligence, planning and conducting attacks, communication and propaganda. They consider that information warfare, which includes but is not limited to cyberterrorism as defined by Devost, Houghton et al. (1997), is a threat to US national security but, contrary to Devost, Houghton et al., believe that terrorists are more likely to use IW techniques in conjunction with conventional attacks in order to compound their effects. In contrast with the genuine threat from these blended attacks, the threat from 'pure' cyberterrorism should not be exaggerated. They see no evidence that terrorists currently intend to engage in IW, but they agree that increasing dependence of the US on interconnected, networked information systems makes it more likely. They expand on the theme of asymmetry, introduced by the comparatively greater reliance of a Western state on its networked systems when compared with the terrorists' own, more modest, requirements. US information systems tend to lack redundancy for economic reasons and may be dependent on a limited number of critical nodes. An attack could inflict considerable damage whilst the modest systems of the attacker are relatively easy to defend. Moreover, Cilluffo and Gergely note the low number of critical assets in infrastructure systems and conclude that, for this reason, there is a low probability of damage during an untargeted attack, such as a natural disaster, and a correspondingly high probability of extensive damage during a targeted attack from an intelligent adversary. Devost, Houghton et al. reply (1997a) that "such a linear, proportional causality analysis is rarely applicable to complex information infrastructures" and relatively minor, untargeted incidents can cause extensive damage. Conversely, they would not exaggerate the importance of cyberterrorism as a *strategic* technological threat to national security.

What is interesting about the reasoned action model so often used in the literature to predict terrorist interest in cyberterrorism is that it flies in the face of traditional views of terrorists as irrational fanatics. Such irrationality is often assumed in religious extremists who tend towards the suicide attacks characteristic of modern terrorism, whose theology is considered alien and not understandable (Mahmood 2001). Yet these

very extremists, particularly the al Qaeda network, are the ones acknowledged to be making the greatest use of ICTs for communication, administrative and planning purposes and the ones most commentators suspect of actively pursuing a cyberterrorist agenda because it apparently makes sense for them to do so.

Denning (2000) has assessed the potential of activism, hacktivism and cyberterrorism side-by-side. Interestingly, she found that activism – that is normal, non-disruptive use of the Internet in support of an agenda or cause – has proved by far the most influential mechanism for influencing foreign policy, citing successful campaigns against the Clipper chip, US cryptography policy and the international campaign to ban landmines. These methods are most effective when used to supplement traditional forms of activist activity. Hacktivism, on the other hand – website hacks, virtual sit-ins, viruses and worms – achieves high levels of publicity for activists and their causes, a fact which was used to good effect by the Mexican Zapatistas, but has rarely had much influence in changing government policy. At the far end of the scale, it is impossible to measure the impact of cyberterrorism on foreign policy since it has never been tested. However, Denning finds that the threat of cyberterrorism has motivated government critical infrastructure protection initiatives at both national and international levels.

On Denning's analysis, to the extent that terrorist organisations are motivated by the desire to promote their cause rather than a desire for mindless violence, rational choice theory might suggest that terrorist Internet activities are more likely to migrate towards the activism end of the scale, consolidating their propaganda efforts and recruiting new supporters to the cause, rather than towards the destructive end of the scale which is more likely to result in the hardening of both potential targets and hearts. This analysis has some support in the literature, with claims that terrorists are most likely to take advantage of public disaffection with the counter-terrorism messages promoted by Western governments and are turning to the Internet for less biased, uncensored accounts of world events. If terrorists are accomplished in the art of spreading propaganda via the Internet, they have an opportunity to manipulate public perceptions and opinions (Stanton 2002).

Some scholars have attempted more holistic models for cyberterrorism. Kshetri (2005) has constructed a framework for understanding global cyber-attacks which, in theory, would encompass terrorist cyber-attacks. The framework highlights characteristics of the attacker, his environment and the victim. Kshetri notes a number of variables contributing to the likelihood of an attack, including the regulatory, normative and

cognitive aspects of the national environment, the skills of the hacker, the motivations for the attack, whether the attack is targeted or opportunistic and, finally, the profile of the target organisation. His framework highlights ideology as part of the cognitive institutions which are associated with national culture, affirming that Islamic ideology has already motivated a number of low-level cyber-attacks, mostly hacktivism. Terrorists, however, are unlikely to be motivated towards opportunistic attacks which may go unnoticed and are more likely to attempt targeted, symbolic attacks with obligation- or community-based motivations. Nevertheless, the aspect of the framework relating to hacking skills suggests that sophisticated skills are required to effect a targeted hack and, accordingly, the probability of a terrorist cyber-attack is much reduced.

Valeri and Knights (2000), arguing from an offensive information warfare perspective, find it more probable that terrorists would choose to manipulate or exploit data within information systems – a semantic attack – with the specific objective of undermining the perception of trust which necessarily underlies all commercial and social transactions online, rather than targeting the CNI directly. This, they argue, would strike right at the heart of the Internet's success, including its social systems and e-commerce (see also Smith 2002). They, too, note that an attack on the CNI is complex operationally because the topography of networked communications and the CNI is difficult to map making targets difficult to locate. Successful, targeted system intrusion would require considerable skill, time and patience. In addition, governments are investing heavily in risk avoidance technology and procedures for the CNI.

Other studies have supported this view, finding that, whilst computer networks may be vulnerable to attacks which are damaging to the economy, the CNI is distributed, diverse, redundant and self-healing, with periodic, accidental outages being relatively routine and easily dealt with (Lewis 2002). Government is ahead of the private sector in terms of information security and risk avoidance for potential government and military targets. Most key systems, particularly the supervisory control and data acquisition (SCADA) systems, are isolated from the Internet and even from internal networks (Green 2002). In contrast, e-commerce ventures in private hands employ the cheaper and less complex option of risk management so that such targets are rather easier to attack. Valeri and Knights' argument is that, by systematically attacking these ventures, they can undermine the perception of reliability and trustworthiness of Internet ventures, cause economic losses, and thereby indirectly affect the CNI by harming

public trust in the Internet in general. This thesis is difficult to sustain six years after publication, trust in the Internet having survived the negative publicity of Y2K, various destructive worms and viruses, high-profile thefts of credit card details and attacks on the DNS.

In sum, the bulk of the literature in this area is speculative, some of it carefully reasoned, some of it less so. The evidence so far is that terrorists make plentiful use ICTs but have not yet engaged in cyberterrorism (Ronfeldt 1999; Whine 1999; Whine 1999a; Arquilla, Ronfeldt et al. 2000; Denning 2000; Green 2002). Nevertheless, reports that cyberterrorism exists or is imminent are legion – from the media, consultants, 'experts', information systems security specialists, law enforcers and politicians – so that the motives behind such claims must be suspect. Commentators have reasoned that such claims are made for ulterior motives such as news circulation, pitches for increased budget or widened remit, and promoting sales of information security products or services (Shockwavewriter 2000). Others have noted that the gap between what is technically feasible and what has actually happened is very large (Denning 2000; Post, Ruby et al. 2000).

6. RISKS AND RESPONSE: THE INFORMATION SECURITY PERSPECTIVE

There is a plentiful information security literature dealing with cyberterrorism, but it tends to be rather one-dimensional and it is almost entirely found in article form, the subject of cyberterrorism not yet having reached major information security textbooks (Prichard and MacDonald 2004). There is also a large practitioner literature, comprised of corporate white papers, conference proceedings and articles in trade journals. The analysis presented in these bodies of work tends to converge around technical possibilities, and intentions and motivations of terrorist organisations are considered only as a function of this: an attack on air traffic control systems is technically possible and the outcomes are potentially devastating, so terrorists must be considering it (Crilley 2001; Kovacich and Jones 2002). The views presented, particularly in the practitioner literature, are often alarmist and these are the views most widely represented in the media (Shockwavewriter 2000; Brunskill 2002; Embar-Seddon 2002).

An element of future-gazing was apparent from the early 1990s. Commentators on information security started looking for future issues and seem to have assumed that cyberterrorism was both a natural progression in terms of seriousness of information security attacks and a natural progression in terms of terrorist activity. It was claimed

that terrorists would turn to cyber-attack and that they were already using well-known hacker exploits (Forcht and Pierson 1994; Furnell and Warren 1999). Such thinking is still current in the literature to a large extent and there seem to be two major approaches. In the first approach, the benefits to terrorist organisations of using the Internet are considered to be overwhelming evidence in themselves that cyberterrorist attacks are inevitable (Furnell and Warren 1999; Crilley 2001). The second approach highlights society's dependence on ICTs and argues that this dependence must make us vulnerable to cyber-attack from terrorists (Furnell and Warren 1999; Griffith 1999; Crilley 2001). Often, no thought is given to the difficulties of attacking specific targets and attacks are described in general terms with the reader left in no doubt about the terrible consequences (Crilley 2001; Kovacich and Jones 2002).

Terrorist use of the Internet is often confounded with cyberterrorism (Furnell and Warren 1999; Hinde 2000; Shockwavewriter 2000; Crilley 2001). Some commentators even label ordinary hacking 'cyberterrorism', applying that alarmist label for impact in much the same way as do the news media (Griffith 1999; Hinde 2000; Ballesteros 2001). Whilst it is often the case that low-level attacks and basic disruption are relatively easy to perpetrate and require minimal skill (Hinde 2000; Paul 2001; Brunskill 2002), some argue that it is not valid to extrapolate from that position and assume that high-end attacks on CNI with catastrophic consequences are similarly easy (Lemos 2002), as others have done (Dwan 2001; Lawson 2002).

A few have effected a more nuanced analysis, explicitly noting the difference between hacktivism, other low-level hacker activity and cyberterrorism (Jordan 2001). Similarly countering the scaremongers, Pollitt (1998) notes that attacks on the CNI are likely to cause most damage but that the impact is rarely likely to be serious or fatal because such systems are usually mediated by human beings (also Green 2002; Neville-Jones 2003). He considers it essential that this element of human mediation in critical processes is maintained for security reasons.

The immediate aftermath of 9/11 saw an explosion in the number of articles written by information security experts, industry and academic alike. There was a sense amongst security professionals working within organisations that there was a window of opportunity for taking advantage of heightened management concern (Cresson Wood 2001; Harreld and Fonseca 2001; Rombel 2001; Senia 2001). Despite claims that information security was a high priority for top management in 75% of businesses (PWC/DTI 2004), this concern did not translate into increased spending and

management reverted to traditional imperatives for return on investment (Brunskill 2002; Schultz 2003) or simply did not agree that the threat had heightened and the extra cost was justified (George and Whatford 2002). Some security professionals were also wary of over-hyping a threat which had yet to materialise for fear of losing credibility at board level as some felt they had done with the Millennium Bug (Schultz 2003). Security vendors also saw economic opportunity at a time when businesses were keeping a tight rein on IT budgets. They saw an opening for the industry in the shape of governments who were ready to open the public coffers for massive investment in the prevention of cyberterrorism and in other technologies needed to fight lengthy wars on foreign soil (Rombel 2002; Williams 2002).

Commentators post-9/11 highlighted the potential for cyberterrorist attack (Boni 2001; Brull and Wagley 2001; Hinde 2001; Brunskill 2002; Kovacich and Jones 2002; Foltz 2004), particularly as a retaliatory measure resulting from Allied attacks on Afghanistan and in Iraq (Hinde 2003). Many contributions were speculative and alarmist rather than rigorous, but some attempted a more structured analysis. Vatis (2001) made a systematic predictive analysis of the kinds of attacks which might be expected during the War on Terror. Although he considered the CNI a target for cyber-attack by terrorists, nation states and anti-US hackers with catastrophic consequences, a close reading of the analysis reveals that much of the activity anticipated really amounted to low-level nuisance, such as website hacks. In the event, a spate of reciprocal hacks did take place, mostly amounting to website defacements (Cover Story 2001), but nothing more serious.

Other attempts have been made at structured approaches to risk analysis, mostly from a technical perspective. Desmedt (2002) noted attempts to identify the most critical infrastructures, a controversial question in itself, and the rather older, larger body of work on establishing cyber-vulnerabilities. He discussed ways of integrating these approaches, underlining the risk that information security alone will not be a complete answer in the event of a physical or blended attack (see also Gordon and Ford 2002).

A few months after 9/11, however, many experts were beginning to reassess their initial claims, acknowledging that destructive cyberterrorism was theoretically possible but convinced that it was infinitely more complex and much less cost effective for terrorists than they had once feared (Lemos 2002; Harper 2003; Simpson 2003). The major types of attack or misuse experienced by organisations have, for many years, been viruses,

insider abuse of Internet access and laptop/mobile theft, in that order (CSI/FBI 2005), and cyberterrorism does not feature at all.

If the claims were initially overblown, the professional advice, aimed mostly at the private sector, was sound. Whether the source of an attack was terrorist or criminal, some argued that the effects on the target would substantially be the same and preparation was essential (Hinde 2003). Information systems vulnerabilities tend to correlate with the level and type of threat, since news of a vulnerability tends to spread fast and exploitative actions can be engineered rapidly before system administrators either know of the vulnerability or have time to patch it (Brunskill 2002). Many commentators urged governments and industry alike towards comprehensive security policies (Bray 2002; Middlemiss 2003), with rigorous risk assessments, threat monitoring, tightened security measures and top-level personnel taking responsibility (Boni 2001; Cresson Wood 2001; Harreld and Fonseca 2001; Hinde 2001; Kirk 2001; Rombel 2001; Vatis 2001). Still, only a third of UK businesses had a security policy in 2004 (PWC/DTI 2004).

Many organisations caught in the destruction of 9/11 had reason to be grateful for lessons learned in preparation for the Millennium Bug (Seifert 2002) in terms of the importance of disaster recovery and contingency planning, as well as the availability and desirability of insurance against cyber-risks (Boni 2001; Brull and Wagley 2001; Kirk 2001; Marlin 2001; Keegan 2002; Leivesley 2002; Smith 2002). Nevertheless, 75% of organisations still do not have external insurance against cybersecurity risks (CSI/FBI 2005). In purely technical terms, the desirability of redundancy, networked communication technologies and approaches to robust, secure, distributed computation have also been highlighted (Desmedt 2002; Seifert 2002). The importance of sharing threat and incident data has been emphasised (Boni 2001; Brunskill 2002), both through national infrastructure protection centres, such as the US NIPC and the UK NISCC, and with industry cooperatives. Indeed, Microsoft and other IT giants set up the Information Technology Information Sharing and Analysis Center following 9/11 (News 2001). Information sharing within industry does seem to be taking off, although reporting to law enforcement and legal counsel is declining. Fear of negative publicity and losing competitive advantage remain the major reasons for this decline (CSI/FBI 2005), although another survey found that the incidents were too small to report or that they were not even criminal (FBI 2005).

Insiders have also been identified as the most likely and threatening of potential attackers (Brull and Wagley 2001; Hinde 2001), either working on their own or as agents of a terrorist organisation (Vatis 2001). Behavioural profiling is increasingly being used to evaluate this problem within organisations (Shaw 2006). In addition, one of the biggest problems facing organisations directly affected by 9/11 was replacing skilled staff, not reinstating damaged technology (Cresson Wood 2001). Consequently the wisdom of concentrating key staff in one geographical area has been challenged (Smith 2002). Yet, if personnel are part of the problem, they are also part of the solution. All personnel coming into contact with company information should be informed and responsible and it is no longer sufficient to concentrate information security in the hands of a few, dedicated professionals.

7. THE INSTITUTIONAL RESPONSE

The institutional response occurs at the national, organisational and international levels and the response at each level is connected to the others. Rathmell (1999) identifies three key assumptions which have become conventional wisdom amongst governments: first, that the government, military and commerce must embrace the information revolution in order to remain competitive politically, economically and militarily; second, that government and defence information infrastructures are a requisite part of the National Information Infrastructure (NII) and that e-commerce should be promoted through technological and regulatory measures; and, third, that government and the NII must be secured against low level attacks and, in the event of a major strategic attack, core activities must still function. Individuals and corporations are expected to protect themselves against routine threats, ensuring reliable and efficient functioning of the e-environment and protection from 'normal' misuse and abuse. On the other hand, the protection of the NII from the lower probability but high-level attacks by hostile states and terrorists properly remains the responsibility of the state.

This has given rise to a new approach to Critical Infrastructure Protection (CIP), the concept of which is not new but has been rendered more complex by the evolving information technology element. Rathmell outlines several key problems which relate to CIP generally, whether the source of the threat be terrorists, criminals or hostile states. Highly complex and evolving system interdependencies renders vulnerability analysis extremely difficult. At the same time, assessing and monitoring the level and direction of the threat is problematic because of a lack of reliable data and the dynamic nature of the threat. Data tends to be unreliable because of under-reporting from

organisations due to lack of monitoring systems and reporting procedures and also the reluctance of commercial organisations to admit to weaknesses in security. Prediction of the threat is even harder so that "some agencies have rejected threat-based approaches in favour of vulnerability-based approaches". The issue of CIP has also intensified the security v liberty debate, best exemplified in the cryptography policies adopted by the US in the late 1990s. In this context, Hosein and Whitley (2002) have also noted that cryptography policy necessarily impacts on ecommerce too, a fact which was recognised in the UK before the debate moved on to national security – in the US, the debate happened the other way around. Importantly, there are also controversies surrounding the definition of the CNI – what is critical and to whom? Finally, Rathmell identifies problems of coordination, control and influence of vertical government structures over networked threats. This last problem has many facets, many of which exemplify the general problems posed by netwar to traditional, hierarchical government and they can be analysed at the national, public-private relationship and international levels. This will be the focus of the next three sections.

7.1 National challenges

(a) Structural issues

Advancing technology can be extremely disruptive of the status quo, often leading to governments attempting intervention (Hosein and Whitley 2002). The first category of problems relates to the intra-government environment since information security issues cut across the responsibilities of so many different departments (Rathmell 1999). The authorities are concerned about emerging modes of operation of their opponents as much as the attacks themselves. Returning to Arquilla and Ronfeldt's concept of netwar (1999), they argue that, since netwar operates outside the traditional societal structures, it is challenging epistemologically the very structure of governments and society itself.

> A netwar actor may aim to confound people's fundamental beliefs about the nature of their culture, society, and government, partly to foment fear but perhaps mainly to disorient people and unhinge their perceptions. This is why social netwar tends to be about disruption more than destruction. The more epistemological the challenge, the more confounding it may be from an organizational standpoint. Whose responsibility is it to respond? Whose roles and missions are at stake? Is it a military, police, intelligence, or political matter? When the roles and missions of defenders are not easy to define, both deterrence and defence may become quite problematic. (Arquilla and Ronfeldt 1999)

This certainly highlights concerns noted by other scholars. Contemporary use of the Internet could be viewed as challenging the structure of society by forcing its members

to think and act in different ways. The major western democracies lack a national strategy and current laws and enforcement structures lack coordination and are largely ineffective against the perceived threats from networked organisations making full use of networked technologies (Gilmore Commission 2000).

Devost, Houghton et al. (1997; 1997b) assert that cyberterrorism is a legitimate concern for law enforcement, the intelligence community and the military, none of which is currently capable of responding individually to the cyberterrorist threat. They call for a new agency covering the related problems of drug enforcement, counter-terrorism, international organised crime and information attack mitigation. This agency would have power to draw upon and coordinate law enforcement, intelligence and military resources as appropriate. They also advocate the creation of units with an offensive capability which would involve detecting, locating and countering cyberterrorists. Strikes would be authorised by the US government, but would be executed so that the government would be able to deny involvement.

Such proposals make uncomfortable reading for those concerned with democracy and the rule of law. Cilluffo and Gergely (1997) consider that the proposed agency would be overwhelmed with information and functionally useless. In addition, the functions ascribed to the proposed offensive units are probably illegal and might constitute an act of war. They prefer the approach of a national information assurance policy on which reasonable, protective information security measures would be based. They also advocate intelligence-gathering, the better to understand terrorist use of information warfare, which includes cyberterrorism; establishing a warning and crisis management centre; and creating national strategy and response options to guide retaliation in case of cyber attack.

These proposals are akin to what was eventually proposed by the US Gilmore Commission (2002) in its vision for a national counter-terrorism strategy. This included a National Counter Terrorism Center (NCTC) which would assume responsibility for intelligence and threat assessment; enhanced powers for the Department of Homeland Security (DHS), which would be able to commission intelligence collection and analysis, and combine threat assessments generated by the intelligence community and the NCTC with its own vulnerability assessments on the US CNI; clear lines of responsibility of the DHS and other Federal agencies before, during and after an attack on the CNI; commissioning a comprehensive risk assessment for the CNI, both physical and electronic; and merger of policy development for physical and cyber-security

policy. These proposals effectively acknowledged the difficulties faced by a rigid state edifice in dealing with malfunction in any part of the CNI. Different parts of the infrastructure are increasingly connected and problems in one place will inevitably ripple out to affect other parts of the CNI (Brunskill 2002). No one part of the state machinery is equipped to deal with the consequences of such an event, be it due to terrorist attack or simple malfunction, and lines of responsibility must be clarified in advance.

(b) Legal issues

It is clear that states can and must take action to protect the public against activities which seriously threaten safety and democracy and the UK has elected to address this issue with permanent, rather than emergency, legislation in the shape of the Terrorism Act 2000. There are a number of justifications for this position (Walker 2000). First, liberal democracies are justified in defending their existence and values and defending their citizens' right to life, even if this requires some temporary limitation of civil rights. Second, terrorism is an illegitimate form of political expression and its physical manifestations probably amount to war crimes. Third, terrorism is a distinct form of criminality which presents particular challenges for law enforcers in terms of remoteness and sophistication of the perpetrators, and their capacity to intimidate an audience wider than the immediate targets. These justifications are broadly accepted by the UK government and electorate alike. Walker prefers a permanent legislative code over emergency legislation, which better "reflects the philosophy of constitutionalism and democratic accountability – that the legislature can secure an important input if it can speak in advance in a way which cannot be drowned by the screams of a crisis". The pitfall, of course, is that such permanently available powers will be used too frequently and without proper cause unless proper safeguards are in place. This seems to be a major point of contention with the Terrorism Act 2000, which has certainly been used in inappropriate circumstances, as in the case of Walter Wolfgang, an octogenarian attending the Labour Party conference in 2005, arrested under the Terrorism Act for heckling. There must be concern about the very broad extension to the definition of terrorism under section 1(2)(e) which, in its definition of cyberterrorism, dispenses with the requirement of any physical damage to persons or property. As Walker points out:

> "it is the final decoupling of the Terrorism Act from its historical grounding in Ireland and the consequent impact on the scope of the definition that raises the possibility of the use of draconian provisions in circumstances where ordinary policing and laws could easily respond to isolated and incompetent terrorists."

It has been argued that, as the threat from terrorism becomes increasingly diffused as a result of terrorist use of ICTs, the need for a coherent system of Internet surveillance becomes increasingly urgent (Merl 2001). A central plank of the UK anti-terrorism regime in this context is the Regulation of Investigatory Powers Act 2000 (RIPA), although powers under this Act are restricted neither to anti-terrorism nor to the electronic environment (Bowden 2002). RIPA sets out the circumstances in which law enforcers, intelligence services and, controversially, other agencies can intercept communications, acquire communications data, and require disclosure of encrypted data (not yet in force).

Hosein and Whitley (2002) note that this legislation poses a number of conundrums, many of which were sidestepped or ignored at the time it was debated. First, personal security enhanced by encryption can be inimical to national security, which is challenged by use of the same technology by criminals and terrorists. Second, rapidly changing technology presents a particular challenge for any legislative regime seeking to maintain the status quo in terms of traditional powers of state since a technical circumvention or avoidance of new legislation can often be found relatively quickly. A good example is the use of pre-paid mobile phones to avoid identification through telephone traffic data (Bowden 2002). This challenge was acknowledged in a report of an all-party Parliamentary committee which heard a quantity of evidence advocating a technologically neutral approach to legislation. The committee ultimately recommended that the Home Office keep the efficacy of data retention legislation under review (APIG 2003). Whitley and Hosein have argued elsewhere (2005) that attempting technological neutrality is misguided, since understanding differing technological characteristics is fundamental to any evaluation of the impact of related policies. Third, legislation requiring the production of encryption keys or allowing surveillance of electronic activity increases both costs and risks to citizens and organisations and may seriously impact human rights. Fourth, there is the additional challenge of regulating in an environment increasingly affected by globalisation. Interestingly, whilst they set out a number of options which might have been open to the UK government, Whitley and Hosein state that legislation imposing obligations on individuals and industry was "selected as the only effective way of meeting the interests of the British Government". Clearly, Whitley and Hosein harbour no illusion that governments are acting to secure the safety of citizens rather than their own vested hegemonic interests.

A raft of legislation was rushed through in both the US and the UK in the months following 9/11, much of which granted new powers to law enforcers in the name of enhancing national security, another term for which there is no settled legal definition (Pounder 2002). However, as is often the case with emergency legislation (Walker 2000), powers were augmented at the same time as safeguards were sacrificed. There were, indeed, strong reasons for new surveillance powers, but legislatures were repealing safeguards which had been instituted because of previous abuse (Swire 2001). In the UK, the most notable development was the Anti-Terrorism, Crime and Security Act 2001, Part 11 of which provides for the possibility of blanket traffic data retention by all communications providers who might then be called on by law enforcement and security services to provide that data for analysis in the course of terrorist and non-terrorist investigations. Retention of the content of communications is not within the scope of this law, although law enforcement agencies can apply to monitor content through other, more stringent, mechanisms. Nevertheless, the nature of traffic data is evolving and its distinction from content is being blurred, particularly when a URL will give investigators a very clear idea of the kind of information the object of surveillance is pursuing (Walden 2005). Part 3 of the Act opens wide the possibilities for sharing data, not only between UK agencies, but also with foreign agencies.

Clearly, similar concerns apply as for RIPA: that there are many ways to ensure anonymity in electronic communications, so that the wide powers are unlikely to be effective against determined terrorists or criminals; and these wide surveillance capabilities threaten the privacy, security and freedom of expression of the law-abiding. By way of safeguards, there is a patchwork of privacy legislation which acts as a safeguard against abuse of these powers, but the approach is fragmented and many different public bodies are involved. In addition, the increasing use of the notion of proportionality theoretically provides a restraint on disclosure of communications data and such disclosure should never be arbitrary or unfair. However, these safeguards are reactive rather than proactive and require the data subject to be aware of the surveillance and in a position to enforce his rights against the authorities through the courts (Pounder 2002). Many are concerned that the motivation for such legislation goes beyond counter-terrorism to the ambitions of law enforcement and intelligence agencies to reduce the barriers to terrorist *and* criminal intelligence and investigation (Bowden 2002; Saiban and Sykes 2002).

In the US, law enforcers have access to some potent electronic investigatory powers under the Patriot Act 2001, including use of the Carnivore software, an electronic surveillance tool probably far more powerful than anything available to the UK authorities. The FBI has also developed eavesdropping software, basically a key logger, called Magic Lantern and it is claimed that the National Security Agency operates a transnational electronic surveillance operation called Echelon together with its counterparts in Australia, New Zealand, the UK and Canada (Levin 2002). There has been serious concern in the US over the way in which Carnivore is used, particularly in relation to the vague and alterable audit trails, so that Carnivore could be used for unwarranted surveillance and the trails covered over (Meehan 2001).

RIPA has been held up in the US as a model in this context for how Internet surveillance can be balanced effectively against the protection of civil liberties, especially privacy (Merl 2001), but this account of RIPA ignores the serious civil liberties concerns which have been voiced in the UK. However, it has been pointed out in the US context, which is similar to the UK position, that the privacy situation may not be as dire as many claim. Surveillance powers have certainly been extended and the main casualty has been the information privacy of ordinary citizens. Nevertheless, these are mostly incremental changes in degree rather than kind and other privacy protections have either remained the same or been improved. A long-term trend for incremental changes may still be dangerous but the situation is not, it is argued, at a critical stage yet (Gellman 2002).

As personal information has arguably become less private, government information has become more opaque. The view of national security as an information restriction concept has a long history (Gellman 2002), the Official Secrets Act 1989 being its most obvious expression in the UK. In the US, much government and military information has recently been removed from public access for fear that it might be useful to terrorists looking for intelligence and ways to attack US interests. Much of this information had been in the public domain for many years and was notable for its usefulness to citizens, rather than terrorists. The danger is that, in increasing government secrecy when this is not strictly necessary, the democratic pillars of fundamental openness and accountability will be eroded and citizens will be less informed on the workings of government (Feinberg 2002; Halchin 2002).

Reinares (1998) has warned that incompetence or ineffectiveness of law enforcers, including excessive brutality, detaining innocents and detention without charge, is an

instrumental factor in determining whether or not terrorism takes root in a particular democracy. Rather, the state should be scrupulous in responding to terrorism in a limited, defined and credible fashion, respecting the legal framework. Counter-terrorism measures should be effective without being overly broad so as to affect the general population. As a result of sustained terrorism, society may be willing to accept restrictions on its liberties to ensure the personal safety of its members and the survival of the political system. However, Reinares finds that an excessively repressive and indiscriminate response that fails to distinguish between the terrorists themselves and the society in which they operate serves to alienate significant sectors of that society, turning them against the government, which then affects the government's institutional legitimacy and may win support for the terrorist cause. It has been noted elsewhere (Chermak and Weiss 2005) that police organisations routinely brief the news media in such a way as to maintain their organisational legitimacy. The effects Reinares highlights may be artificially minimised by careful handling of the media who provide an opportunity to shape public understandings of crime in society, promote certain understandings of the police response to crime and generate support for certain policy options. In return, the media gain access to easy and interesting law and order stories for publication.

(c) Strategic issues

The UK Parliament has been advised that the current threat to the CNI from cyberterrorism is low, although the situation is not stable so that policies of prevention and enhancing resilience should be actively pursued (Neville-Jones 2003). Certainly, there is a chance that cyberterrorism will become a reality in the future and the issue cannot be ignored. It is also possible that the Government and security services possess classified evidence about cyberterrorism which has not been put in the public domain. Notwithstanding that caveat, cybercrime, on the other hand, is a real and serous economic threat to society and some argue that society's resources and efforts should be concentrated here (Denning 2000a; Green 2002; King 2003). In so doing, society would automatically be putting itself in a better position to respond to cyberterrorism if it ever materialised. Similarly, Rathmell (1997) urges governments to be proactive in addressing vulnerabilities rather than reacting when or if terrorist groups actually embrace cyberterrorism, noting that the US has started the process of reviewing vulnerabilities (Presidential Decision Directive 63 1998) but that a similar process in the UK lacks government leadership. Others have underlined the dangers in taking disproportionate steps to counter an unknown threat, particularly if the public later

discerns the exaggeration and grows cynical towards warnings about real threats (Green 2002).

Policy makers and academics alike should be aware of the trap which terrorism sets. Just as the rhetoric of terrorists is used to frighten, persuade and cajole, so too is the counter-terrorist rhetoric, with its good against evil subtext.

> Terrorism is a concept that mystifies rather than illuminates; it is a political and not an academic notion. (Mahmood 2001)

Suspicion is growing that governments are hyping the cyberterrorism threat in order to progress a broader agenda, conveniently ignoring or brushing aside the lack of evidence (Green 2002). The challenge is to peg policies to reality, to acknowledge what is not known, to take sensible, proportionate precautions against what can reasonably be expected and to keep Draconian legislation to a minimum. To react disproportionately to a threat which cannot easily be quantified, thereby eroding fundamental rights of citizens, risks achieving part of the terrorist goal (Embar-Seddon 2002). There are plenty of claims in the media, by politicians, industry insiders and experts, about what cyberterrorists might be able to do (Green 2002; Harvey 2002). Much of this is fanciful and leads a concerned public to imagine attacks rather worse than are realistically possible (Giacomello 2004). Rarely, if ever, do public figures say, "This is what cyberterrorists cannot do". They cannot remotely launch nuclear missiles, since their control systems are isolated from the Internet; nor are they likely to be able to crash aircraft by attacking air traffic control systems, because their systems are mediated by humans, there are contingency plans, redundancy in the systems and pilots rarely rely exclusively on air traffic control (Embar-Seddon 2002; Giacomello 2004); and the breach of a dam, even if it were possible by purely electronic means, would be so much cheaper, simpler and more certain if a conventional bomb were used that no 'rational' terrorist would ever consider the electronic route (Giacomello 2004). The academy has a duty to check government propaganda as well as to correct innocent mistakes and propose solutions (Shneiderman 2002). If such errors are left unchecked, exaggeration of the evil qualities of and risks from terrorists will continue to produce the over-reaction characteristic of counter-terrorism measures which, in turn, risk escalating the very violence they seek to control (Mahmood 2001; Cohen 2002)

7.2 The challenge of public-private relationships

The main target for cyberterrorists is usually thought to be the CNI but detailed vulnerability assessments are usually classified and much of the literature on this

subject is necessarily general or speculative in nature. Much of the CNI, not to mention the health of the economy, is concentrated in the hands of organisations in the private sector (George and Whatford 2002; Rathmell 2003; Cumming 2005), yet counter-terrorism is still perceived as a government function (Farrell 2003). This creates several challenges.

First, privatisation, deregulation and globalisation of many industries and utilities have led to reduced government control over and knowledge of owners and operators of information networks and regulation of the Internet in particular is extremely challenging (Madsen 1996; Rathmell 1999). Fierce commercial competition has also rendered businesses reluctant to work with government, particularly given their desire to avoid any unduly restrictive regulation (Lewis 2005). Many governments and their law enforcement agencies, including those in the UK, are now in the position of wanting to reassert control over the telecommunications networks and are facing an uphill struggle against a public whose imagination has been captured by the perceived freedoms offered by the Internet (Madsen 1996). In addition, the digital network encompasses every online business and individual, so the data required by law enforcers to monitor potential and actual threats is unprecedented in scope (Rathmell 1999). In the UK, this controversial issue was highlighted by the introduction of RIPA, granting new powers of interception of and access to communications data, powers which have subsequently been strengthened by adoption of EU Directives regulating data retention in 2002 and 2005.

Second, legislating for national security often has an adverse impact on commerce generally, because either greater restrictions or onerous duties are imposed (Hosein 2006).

> [Homeland security] policy action is a source of risk itself that must be managed. Policy responses can create their own climate of uncertainty and risk. In the process of developing a coherent vision and policy for its actions both at home and abroad, the US government will inevitably make a number of mistakes of over-reaction, missing opportunities, omission/commission errors and the like. These actions will have consequences for US firms in their international competition. (Spich and Grosse 2005)

The risk is that, in securing the nation against the threats of crime and terrorism, a government may go too far so that market freedoms are adversely affected, commercial organisations are forced to engage in regulatory arbitrage and business is lost to another country (Bowden 2002; Hosein and Whitley 2002). Members of the UK Parliament have already recognised the risk that the substantial costs of data retention legislation in

the UK and across the EU will put European communications service providers at a competitive disadvantage to their US counterparts (APIG 2003).

Third, the private sector must have relevant information and the means of protecting itself in order that both the economy and the privately-owned part of the CNI may remain secure against cyberterrorist attack. The US Gilmore Commission (2000; 2001) has advocated greater cooperation between the public and private sectors to address the problems of both cybercrime and terrorism, proposing that a framework for coordination be developed, including the use of security standards for critical technologies. The Commission (2001) also noted that the US National Infrastructure Protection Center (NIPC), with responsibility for critical infrastructure alert, warning and response coordination, was failing in its duties partly because it operated from within the FBI, thus encouraging a belief that the NIPC had more to do with law enforcement than information sharing. It was seen as extremely important that the NIPC be seen to represent all stakeholders, public and private alike.

In the UK, the National Infrastructure Security Co-ordination Centre (NISCC) was founded in 1999 with the remit of identifying the electronic CNI, threat assessment, outreach to private organisations, response, research and development. This is an inter-departmental government centre which coordinates input from many parts of government: defence, trade, Home Office, intelligence services, central policy and law enforcement (Cumming 2005). Part of the NISCC's remit is to coordinate this government expertise with that of the private sector. In addition, they promote information sharing within industry. Early attempts to establish an Information Sharing and Analysis Centre within the IT communications sector failed because of an unwillingness of commercial organisations to divulge information on the existence and severity of successful attacks (Brunskill 2002). However, as part of its strategy to protect the UK's CNI from electronic attack, the NISCC is now promoting information sharing in tandem with the Central Sponsor for Information Assurance and provides assistance in setting up Warning, Advice and Reporting Points (WARPs). WARP members agree to work together in a specific community, perhaps based on a business sector, and share information to provide early warning of alerts and vulnerabilities, thereby reducing the risk of their information systems being compromised. Strategies such as these are also important in order to distinguish patterns in cyberattack which may prove helpful to security efforts (Kjaerland 2006).

There is a good deal more work to be done to coordinate the UK authorities' cooperation with the private sector and there are significant barriers. First, there are numerous relevant government agencies whose remits overlap and their rôles are very confusing at the interface with the private sector. There is a need to share resources and information, not only between the public and private sectors (Devost and Pollard 2002), but also between public agencies who have a tendency to defend their turf. Second, public and private organisations need to cooperate but have very different priorities, the former being process-driven and the latter outcome-oriented. This has historically led to wariness and lack of a common language and understanding. Third, the public sector needs to encourage the IT industry to build in security features, yet there is often little commercial incentive to do so. Fourth, further attempts must be made by the public sector to encourage information sharing within the private sector and find a way to overcome the trust, confidentiality and competition issues which have historically formed a barrier to success. This is the Holy Grail for public-private cooperation and probably the hardest of all the goals to achieve (Brunskill 2002).

A 2004 survey found that half of large UK businesses respondents drew on government security guidelines (PWC/DTI 2004), suggesting that government has the potential for positive influence through careful guidance as an alternative or in addition to formal regulation. Lewis (2005) disagrees and has argued in a US context that the government's cyber-security policies based on market forces and voluntary cooperation of the private sector are perverse in the heightened security environment post 9/11. He argues that defence and security are public goods which the market will never supply in sufficient quantity. Ironically, one of the major barriers to sensible government regulation has been the over-hyping of the cyberterrorist threat which has given the impression that regulation of the private telecommunications sector would need to be extensive and, inevitably, very costly. By mapping the CNI and grading the importance and vulnerability of each element, Lewis proposes a model for minimal government interference in the market whilst still ensuring suitable levels of security through achievable levels of regulation in the most critical areas. Crucially, this involves abandoning crude 'electronic Pearl Harbor' scenarios.

As well as assisting government to defend national infrastructures and pursue terrorists through data retention, commercial organisations must also attend to the terrorist threat they face themselves (George and Whatford 2002; Leivesley 2002; Smith 2002; Veness 2002). There is evidence that al Qaeda associates have considered corporate targets as

part of a general campaign against Western economies (Davies 2002). The private sector must minimise the impact of terrorism on their own organisations and thereby on society as a whole (Bray 2002). All industries are implicated, of course, not just the telecommunications sector. The FSA, the UK financial services regulator, has noted that terrorist finance poses significant danger to the reputation of UK financial markets. The international and domestic counter-terrorist financing regime is designed to make operation in the financial environment for terrorists and their financiers difficult by increasing both the costs and risks for these groups (FSA 2006). Others have characterised terrorism as a market imperfection, increasing transaction costs, creating a barrier to the free flow of goods and hindering potential gains, all of which calls for specialised marketing strategies to prevent consumer drop-off (Czinkota, Knight et al. 2005). High levels of outsourcing arrangements are the norm in both public and private sectors, particularly in the field of information and communications technologies, resulting in many-to-many relationships which often have networked information infrastructures. A successful attack on one organisation therefore has the potential to affect many contractual partners. Similarly, a successful information security strategy will involve a coordinated response from a number of different organisations (Brunskill 2002).

7.3 International challenges

The threats and vulnerabilities relating to cyberterrorism and other security risks are transnational, as evidenced by the ripple effects across the globe after 9/11 in economic, political, social and psychological terms (Rathmell 2002). This means that any successful solution requires international cooperation on CIP (Rathmell 2003), but Rathmell (1999) has noted a number of barriers. The first issue is that governments prefer to establish their national arrangements before attending to international cooperation and the domestic challenges are legion. Governments recognise that they cannot work in a vacuum but international cooperation is considered a challenge too far for now, leading to an ad hoc response based on existing international structures. These rely on bilateral security and intelligence cooperation, such as the strong ties which exist between the US and UK; multilateral fora such as the G8 and EU; and international information security standards, such as ISO17799.

The concept of transnational risk is best characterised by the fact that online deviance routinely has its source in one country and its target in another. This creates problems with enforcement and prosecution of the criminal law which is, traditionally, territorial

in nature. There are, however, four generally recognised principles on which extraterritorial application of criminal law will be tolerated, relating to nationality of the perpetrator, nationality of the victim, crimes against humanity and safeguarding the national interest. Indeed, the trend in the UK for provisions relating to cybercrimes and terrorism is towards specific provision for extraterritorial application in the relevant legislation. But national legislation with extraterritorial application is only helpful if such laws can be pursued and enforced with the cooperation of other states. In the context of cybercrime, much good work has been done in the Council of Europe and by the OECD, which may indicate a way forward for similar work on cyberterrorism. The importance of the Council of Europe's Convention on Cybercrime is that its signatories include, not only the majority of CoE members, but also the US, Japan, South Africa and Canada. This provides much-needed harmonisation of the response to the security threat posed by criminal and terrorist networks in cyberspace (Walden 2005).

A second issue is definitional in nature (Rathmell 1999; Rathmell 2003): how the problem is characterised dictates which international fora are appropriate. If the threat is defined as being from organised crime, hackers, corporate espionage and sub-state terrorism, then the threat is to the economy and social stability. In this paradigm, all nations have an incentive to work together, drawing on a range of technical, policy, legal and law enforcement mechanisms. If the threat is defined as being from nation states and focuses on IW and information operations as tools of strategic coercion, covert action and espionage, then the solutions are found in international approaches to arms control and the laws of armed conflict. This approach is highly problematic because imperatives of national security and intelligence mean that states want to retain their IW capabilities. The international tension surrounding these issues was nicely highlighted by the Russian UN General Assembly resolution proposing arms control approaches and calling for an "acknowledgement that the use of information weapons against vital structures is comparable to the consequences of the use of weapons of mass destruction" (UNGA 53/70). The resolution was ultimately buried as a result of some neat procedural manoeuvres by, primarily, the US.

From a legal perspective, Dartnell (1999) has noted that the lack of an international consensus on the definition of terrorism accounts for the weak international response to counter-terrorism. Identical arguments apply to cyberterrorism and cybercrime. He criticises this state of affairs, noting that failure to define terrorism may lead to abuse in both directions when the question arises of whether an offence is political or non-

political. The loose frameworks established by the current conventions leave a wide discretion to individual states and a lack of due process provisions can lead to further abuse, undermining the international order. Dartnell advocates perseverance at the international level, however, because "international conventions on terrorism embody 'positive globalization' by broadening the imperative to not inflict physical harm on peoples or materials with whom one might not share bonds based in a political or other type of community." The international effort should focus on violence as a by-product of multiple interests, values and experiences which produce conflict. Once terrorism is viewed this way, Dartnell argues, policy makers are liberated from ideology and can base international laws on "management models or relational-based concepts rather than notions of 'order' that do not correspond to the inter-network character of contemporary global societies, economies, politics, technologies and cultures." Hence, a global legal framework should, first, deal with the substantive causes of conflict in an attempt to remove the reasons for terrorism and, second, address the means of coercion and destruction. The mechanisms for international co-operation established, it would fall to individual states to elaborate further levels of governance.

International agreement on regulation of any issue related to the transnational phenomenon of the Internet is fraught with problems because of the vested interests of each state involved. The Internet is global and states are territorial, so that conflict in any international debate on regulation is almost guaranteed. Moreover, at the international level, politics are even further removed from the public interest, with states being more concerned with protecting and extending their own powers. Any balanced and informed approach to regulation at this level would have to involve stakeholders from many different sectors: public, business, technical communities, human rights organisations. The list would be long and the negotiations unwieldy, but truly *public* policy on Internet-related issues should not be the exclusive preserve of governments (Internet Governance Project 2005).

8. THE PUBLIC RESPONSE

There are no authoritative surveys available which deal specifically with public attitudes to cyberterrorism. There are some industry surveys about attitudes of information security professionals to the threat from cyberterrorism, but they are difficult to evaluate because the term is never defined. For example, one survey found that pre-9/11 22% were very concerned about cyberterrorism whereas, one year later, 48% claimed to be very concerned, with 4% claiming their companies were less concerned than they were

in 2001 (M2.com 2002). Two years after 9/11, a survey of 725 cities conducted by the National League of Cities found that city officials ranked cyberterrorism alongside biological and chemical weapons at the head of a list of fears (Green 2002). Another survey claimed that 49% of respondents consider cyberterrorism a bigger threat than a power outage or natural disaster (CIO Insight 2004). In each case there was no clear indication of what exactly constitutes 'cyberterrorism' and the results suggest a broad interpretation.

The latest available UK information on attitudes of the general public towards technology crime generally is found in the British Crime Survey 2002/3, a victimisation survey, and the Offending, Crime and Justice Survey 2003, a self-report offending survey (Allen, Forrest et al. 2005). 46% of BCS respondents (aged 16-65) had personally accessed the Internet, compared with 71% of OCJS respondents (aged 10-65). Of BCS respondents who used the Internet, 49% had used a payment card for online purchases and, of those who had not, 41% said they would consider it. Of those who had used payment cards online, 75% were concerned about the security of doing so. 35% were worried about giving personal details online. This compares with a more recent survey finding half of active Internet users are 'extremely' or 'very' concerned about the potential fraud risk of making an online transaction (FSA 2006). 74% of BCS respondents who shopped online looked for secure sites as a primary precaution and around half said they would only shop from reputable companies, recommended or well-known sites. Despite these worries, only 1% (n=86) of OCJS respondents admitted any kind of card fraud and, of these, only n=4 admitted to accessing card details online.

Only 18% of BCS households accessing the internet reported a computer virus infection for the previous 12 months and only a third of these reported the problem. Less than 1% of OCJS respondents admitted to sending out a virus in that time. 2% of BCS households accessing the Internet thought someone had hacked into their files in the previous 12 months and less than 1% of OCJS respondents admitted to hacking activities. One third of Internet users were worried about accessing or receiving offensive, pornographic or threatening material over the Internet, and one fifth had actually done so, but only 18% reported it. Most worries seem to be connected with children in the home and pornography.

None of these figures suggest panic about online deviance generally, let alone cyberterrorism. Respondents may be concerned about credit card fraud, but this does

not stop them shopping online. The low numbers reporting problems with viruses, hacking and offensive material and even lower numbers sufficiently concerned to report problems suggest that people are relatively comfortable with their everyday use of their home computers. The online market is currently the fastest growing sector of UK retail. Consumer confidence and expectation is increasing and one in four consumers now purchase goods online, with 14.6 million online shoppers in 2005 (Verdict 2006). Of further comfort is the fact that, of OCJS respondents, less than 1% admitted to visiting a racist website and less than 2% had visited a site giving details on how to commit a crime. This would appear to answer in some measure the fears of those who are concerned that large numbers of individuals will be drawn to terrorist websites and look for ways to commit cyberterrorism.

Allen, Forrest et al. (2005) point out that there is very little known about public attitudes to these issues and the BCS is the first large-scale household survey to cover them. There is certainly no major research into public attitudes towards cyberterrorism. Established annual surveys, such as those produced by the CSI/FBI in the US and PWC/DTI in the UK, concentrate on organisational respondents and survey only criminal breaches of security for the very good reason that these are what victim organisations are routinely experiencing. There is an urgent need for scholarly research on attitudes of the general public towards hacking generally and cyberterrorism in particular.

9. SOCIAL REACTION TO CYBERTERRORISM AND THE POWER OF DEFINITION

There is power in a name. Careless use of terminology impedes understanding, flow of ideas, sense making and policy decisions (Desouza 2005). Forming policy to counter a phenomenon which is insufficiently understood may result in rules which either do not address the issue adequately or overextend the law into areas where it is not warranted (Walden 2005). The literature summarised in this chapter highlights many of the consequences of characterising an action as 'terrorist' in the information environment. The dramatic associations of terrorism may inspire fear and apprehension and the public are led to fear the worst: whether they follow that lead is a separate question. Governments resort to Draconian policy measures, often involving infringements of civil liberties of both suspects and the wider population which are justified by the extreme nature of the threat they are intended to counter. Military and intelligence services, as well as police, become involved and counter-terrorist operations take on a

quasi-military character. Very large sums of money are expended on prevention measures, counter-intelligence and investigation in both the public and private sectors (Giacomello 2004). Social stigma attaches to those labelled 'terrorist', their cause, their methods and their associates.

This last point leads to a perspective largely absent in the cyberterrorism literature: that of the social scientist. Outside the political science field, social science studies on terrorism generally are rare enough (Ballard, Hornik et al. 2002) and the social science literature on cyberterrorism is even more restricted. Current research is uncoordinated and fragmented and cross-disciplinary studies are unknown (Desouza, Koh et al. 2006). This accounts for the rather one-dimensional approach in the literature reviewed in this chapter. A rigorous assessment of cyberterrorism from within the social science domain is long overdue and would add significant clarity to future debate. As Becker says:

> What can social science contribute to understanding and solving any social problems? It helps in several ways: (1) by sorting out the different definitions of the problem; (2) by locating assumptions made by interested parties – assumptions belied by the facts; (3) by discovering strategic points of intervention in the social structures and processes that produce the problem; (4) by suggesting alternative moral points of view from which the problem area can be assessed. (Becker 1966: 23)

This study aims to proceed a little way along the path outlined by Becker. Cyberterrorism is a peculiar case of a problem being defined without any significant underlying empirical evidence to substantiate it. It is a problem based on assumptions, namely that ICTs can easily be used to achieve destructive outcomes and that terrorists are inexorably moving towards this sphere of operation. Governments, agents of social control and industry stakeholders are constantly seeking ways of preventing or mitigating the problem. Finally, perceptions of cyberterrorism are overwhelmingly technical and the military perspective is dominant. Alternative conceptions of the problem are urgently needed in order to build a multi-faceted understanding of the social response.

As concern about the scope of counter-terrorism measures in the UK grows, it is vital to understand the definitions of cyberterrorism being used to justify some of these measures. The wider the definitions used, the greater the encroachment on civil liberties is seemingly justified and the greater the impact on the groups and individuals labelled 'cyberterrorists'. The next chapter will introduce the concept of moral panic which focuses on the definition of deviance as a social process, involving discourses between a variety of stakeholders, including the media. It focuses on the social reaction

to deviance and integrates notions of social control, labelling and deviance amplification in a manner particularly suited to the study of the social reaction to cyberterrorism.

CHAPTER 3

MORAL PANIC: DEFINING DEVIANCE

1. INTRODUCTION

> Societies appear to be subject, every now and then, to periods of moral panic. A condition, episode, person or group of persons emerges to become defined as a threat to societal values and interests; its nature is presented in a stylized and stereotypical fashion by the mass media; the moral barricades are manned by editors, bishops, politicians and other right-thinking people; socially accredited experts pronounce their diagnoses and solutions; ways of coping are evolved or (more often) resorted to; the condition then disappears, submerges or deteriorates and becomes more visible. Sometimes the object of the panic is quite novel and at other times it is something which has been in existence long enough, but suddenly appears in the limelight. Sometimes the panic passes over and is forgotten, except in folklore and collective memory; at other times it has more serious and long-lasting repercussions and might. (Cohen 2002: 1)[1]

This classic formulation of the moral panic appeared in Stan Cohen's book on the social furore surrounding the Mods and Rockers in the 1960s (Cohen 1972). The concept was later comprehensively restated by Goode and Ben-Yehuda in 1994 in "Moral Panics: the social construction of deviance" (Goode and Ben-Yehuda 1994). The models of moral panic provided by each of these texts were then analysed, applied and refined by Chas Critcher in his 2003 book "Moral Panics and the Media" (Critcher 2003). This study draws on these three works to create a framework for analysing the social definition of and reaction to cyberterrorism.

2. MORAL PANIC: AN OVERVIEW

Cohen's classic formulation of a moral panic is by far the most quoted and evokes nicely the social atmosphere characteristic of an archetypal moral panic. Moral panic is an empirically verifiable phenomenon (Goode and Ben-Yehuda 1994: 41) but it is also, more importantly, an abstract model of a process which can be used as an heuristic device so that the emergence of a real-life social problem can be compared with the ideal type moral panic to discover both which elements are present and which are not (Critcher 2003: 2). Such a view of moral panic broadens the spectrum of its application

---

[1] References in this chapter are to the 3rd edition of "Folk Devils and Moral Panics" because this edition contains the important "Introductions" to both the 2nd and 3rd editions, both of which progressed the moral panic debate.

to encompass social phenomena which may not empirically amount to a moral panic but which are, nevertheless, illuminated by rigorous analysis according to the moral panic framework.

Before addressing the specifics of the two models of moral panic used in this study, it is necessary to set out in broad terms the social processes at work during such an episode. Critcher argues persuasively that moral panic has three dimensions (Critcher 2003: 5 and 177): it is a process of definition and action; it marks the moral boundaries of society; and it represents a set of discourses at various levels. Critcher finds that the existing models of moral panic require modification to encompass all three of these elements, since they do not currently deal adequately with the second and third.

2.1 A process of definition and action

First, social problems are viewed as socially constructed, with no necessary connection between the objective nature of the problem and its social definition. Indeed, it is possible to have a moral panic over an issue which, on an objective analysis, does not even exist. Specifically, behaviour is defined as deviant if it is perceived as threatening to certain values or interests of society. The social reaction to deviance thus defined will, in an archetypal moral panic, be disproportionate to the objective nature of the threat.

The central problematic of moral panic lies in this juxtaposition of objective reality with subjective concern or reaction. Waddington has claimed that the concept of moral panic lacks any notion of how the gravity of the phenomenon and the reaction to it might be measured and compared; that the concept is value-laden and lacks objective validity (Waddington 1986). It provides neither the quantitative, objective criteria by which to claim that the reaction is disproportionate to the action, nor the universal, moral criteria to judge that the reaction is an inappropriate response to the moral gravity of the action (Cohen 2002: xxviii).

The response to such criticism exposes the philosophical underpinnings of the concept of moral panic. The constructionist approach adopted is necessarily what has been termed contextual constructionism since moral panic scholars believe the objective dimension is both admissible and empirically identifiable, albeit with difficulty (Goode and Ben-Yehuda 1994: 94). Indeed it must be so if an endless cycle of claims-making and value judgement is to be avoided: strict constructionists would deny entirely the existence of the objective dimension on which the concept of moral panic relies, insisting that the researcher's 'social construction' of the issue is not ontologically

privileged. There is no room for relativism here since the objective dimension provides at least part of the all-important historical context, without which we are unable to answer the questions: why this? Why here? Why now?

More problematic than ascertaining the objective dimension itself is the evaluation of the subjective against the objective dimension. This is not a comparison of like with like. As Cohen says:

> Questions of symbolism, emotion and representation cannot be translated into comparable sets of statistics. Qualitative terms like 'appropriateness' convey the nuances of moral judgement more accurately than the (implied) quantitative measure of 'disproportionate' – but the more they do so, the more obviously they are socially constructed.
>
> The critics are right that there is a tension between insisting on a universal measuring rod for determining the action/reaction gap – yet also conceding that the measurement is socially constructed and all the time passing off as non-politically biased the decision of what panics to 'expose'. (Cohen 2002: xxix)

Perhaps the universal measuring rod is problematic, but nor is it entirely necessary. A common sense approach allows the researcher to view the 'action/reaction gap' as a continuum, with obvious examples of disproportionality/inappropriateness at the centre, and grey areas at the edges. The obvious cases are intuitively so, which does not deny the theoretical force of the criticism, but mitigates its concerns to acceptable levels for practical purposes.

2.2 Marking the moral boundaries

Whilst claims for the empirical verifiability of an underlying social condition may be admissible – and social science research spanning decades has made this assumption – claims that there are universal moral criteria by which to judge the appropriateness of a reaction must surely founder (Ungar 2001). Yet, at any given time and, most importantly, in a given context, one or more dominant moral codes can be identified. Society does produce pockets of consensus which, whilst not universal, represent the views of a significant section of society. In no sense does the concept of moral panic demand a universal moral standard. Rather, it seeks to identify where and how the moral boundaries are drawn and how these are used to influence social outcomes.

During the course of a moral panic, the definition of behaviour as deviant may also involve the identification of specific individuals as wholly responsible and lying outwith the moral boundaries of society. The attributed characteristics of folk devils, in Cohen's terms, are unambiguously negative, even evil. This enables the maintenance of the moral status quo, but may go further so that certain powerful elements in society claim the moral high ground at the expense of those successfully cast as folk devils who lack

the means to fight back. Moral boundaries are, thus, not so much maintained as redefined. Critcher argues that folk devils should no longer be considered an essential feature of a moral panic (Critcher 2003: 151) and his case studies demonstrate how the moral dimension can be applied to the behaviour itself without the successful casting of a folk devil.

2.3 The underlying discourse

The definition of both social problems and moral boundaries is a manifestation of negotiation and struggle amongst and between subcultural groups, and relationships between those with differing relative amounts of political power. Although definitions are very often contested, where agreement cannot be reached, solutions are imposed by those wielding greater political power (Goode and Ben-Yehuda 1994: 82). A discourse can be mobilised and brought to prevail through a clear process of symbolisation, usually through the media, which results in stereotyping the features of deviance and deviants and establishing a "simplified dichotomy between good and evil" (Critcher 2003: 144). Critcher argues that the underlying discourse in many moral panics over recent decades has shifted from a continuing discourse on youth and deviance in the 1960s and 1970s, exemplified by Cohen's Mods and Rockers (Cohen 1972) and Hall's muggers (Hall, Critcher et al. 1978), towards a discourse on children as victims, including concerns about video nasties, child abuse and paedophilia (Critcher 2003: 155). The discourse on youth and deviance persists, of course, and it is pertinent to this study because hacking is perceived as youth deviance. Additionally, the definition of cyberterrorism draws on existing discourses on technology and terrorism.

Cohen notes that a study of crime reporting in Britain has found that there has been a shift in focus from offence, offender and criminal justice system towards victims (Cohen 2002: xxiv). Offenders become easier to demonise if the context of their actions are ignored (motivation, social circumstances etc) so that stereotypes can be drawn without serious contest. Stereotypes are crucial to the demonisation process:

> Moral panics depend on the generation of diffuse normative concerns, while the successful creation of folk devils rests on their stereo-typical portrayal as atypical actors against a background that is overtypical. (Cohen 2002: 45)

Once these targets for social hostility have been set up and made instantly recognisable, demands are made that 'something must be done', with the ultimate aim that folk devils, or at least the identified behaviour, should be eradicated (Cohen 1972: 41-4; Goode and Ben-Yehuda 1994: 28-9). Once a discourse has been established during a moral panic,

its participants are sensitised to the issues and the symbols and stereotypes are available for the future, possibly leading to a serial panic (Critcher 2003: 145).

This account of the importance of the discourses underlying a moral panic is not unproblematic. Arguments about mobilisation of discourses and imposition of a specific definition by the socially powerful imply, and sometimes make explicit, that moral panics are deliberately engineered by the élite for their own hegemonic purposes (eg Hall, Critcher et al. 1978). The counterclaim is that 'moral panic' is a value-laden concept used by leftist liberals and political radicals to condemn the actions of the political élite. As the use of the term 'moral panic' became used in the media itself, it became more common for politicians, first those in the Thatcher administration and later those in the New Labour administration, to reinforce the causal theories which underpinned moral panics and to claim that those using the term 'moral panic' were out of touch with public opinion which was justly concerned about the relevant issue. Blame was laid at the door of "the 'jargon-laden left' for using the term so selectively" (Cohen 2002: xxxii).

Cohen counters (2002: xxxiii-xxxv) that, if the phenomenon just described amount to 'bad' moral panics, then there are also such things as 'good' moral panics, using the social mechanisms identified as constituting moral panics to raise awareness about issues which would otherwise be ignored. From time to time the media attempt to create moral concern in a climate of denial, and Cohen gives the example of work by Moeller (1999) who describes 'compassion fatigue' in relation to the atrocities in Rwanda and Bosnia. He concludes that:

> Sociologists have no privileged status in pointing [social injustice] out and suggesting remedial policies. But even if their role is relegated to being merely another claims-maker, this must include not only exposing *under-reaction* (apathy, denial and indifference) but making the comparisons that could expose *over-reaction* (exaggeration, hysteria, prejudice and panic).

In other words, you cannot have your cake and eat it.

The next sections will consider two models of moral panic, provided by Cohen (2002) and Goode and Ben-Yehuda (1994) respectively, as modified by Critcher (2003). These two models will be used as a framework for this study: Goode and Ben-Yehuda's attributional model to organise the findings and Cohen's processual model to structure the discussion of the findings. In addition, the discussion will pay attention to the elements described in Sections 2.2 and 2.3 which are perhaps not dealt with adequately in the processual model: marking the moral boundaries and the underlying discourse. In

each of the case studies employed by Critcher to assess the usefulness of moral panic as an heuristic device, these elements are discussed in a section entitled "Beyond Moral Panics" (Critcher 2003: 41, 58, 74, 92, 112) and he concludes that the insights gained from this extension of the analysis should be incorporated into any future model of moral panic (Critcher 2003: 177).

Cohen is discussed first in this chapter because his was the first formulation of the moral panic concept.

3. COHEN: THE PROCESSUAL MODEL

In order to elicit what he terms the 'processual model', Critcher draws together three aspects of Cohen's work: the elements in his classic statement (quoted in Section 1), his disaster analogy, and the deviancy amplification model.

What is usually taken to be Cohen's classic statement is not comprehensive, even in Cohen's own terms, notably leaving out any mention of folk devils, control culture and underplaying the rôle of the media, all of which he considered central. However, it does give a sense of how Cohen organised his analysis according to a succession of social processes:

1. A condition, episode, person or group of persons emerges to become defined as a threat to societal values and interests;
2. its nature is presented in a stylized and stereotypical fashion by the mass media;
3. the moral barricades are manned by editors, bishops, politicians and other right-thinking people;
4. socially accredited experts pronounce their diagnoses and solutions;
5. ways of coping are evolved or (more often) resorted to;
6. the condition then disappears, submerges or deteriorates and becomes more visible. (Cohen 2002: 1)

As a framework for his account of the social reaction to the Mods and Rockers, Cohen used an analogy drawn from disaster research, which had identified several sequential stages in public reaction. Cohen distilled these stages into four: warning, impact, inventory and reaction. It is possible to see how this framework can be used to discuss the six elements described above, yet Critcher criticises the analogy of moral panic with disaster as forced because disasters generally lack the moral dimension (Critcher 2003: 11).

Finally, there is Cohen's deviancy amplification model. His work is based on a transactional approach to deviance, according to which deviance is constructed in the course of interactions between the 'deviant' and society. Definitions of deviance and identification of, and reaction to, folk devils are central to a moral panic, even though the existence of a folk devil is not, perhaps, an invariable rule (Ungar 2001; Critcher 2003: 151). Indeed, the concept of moral panic owes a great debt to Howard Becker's work on labelling theory, which encompasses the idea that:

> Deviance is not a quality of the act the person commits, but rather a consequence of the application by others of rules and sanctions to an offender. The deviant is one to whom that label has successfully been applied; deviant behaviour is behaviour that people so label. (Becker 1963)

On this view, the successful labelling of behaviour as deviant and/or the creation of a folk devil occurs only after their identification as threatening to certain social values or interests, setting in motion various societal control responses. In connection with the societal control culture, Cohen describes a process of 'deviancy amplification'. The deviancy amplification model rests on the idea that 'social control leads to deviance' is potentially a richer premise for studying deviance than 'deviance leads to social control' (Lemert 1951; Lemert 1972; Cohen 2002: 6). An initial, social problem leads a sub-cultural group to construct a (deviant) solution which draws a reaction from society in general and the societal control culture in particular. The processes of exploitation and stereotyping which form part of this reaction and the application of the 'deviant' label have the effect of isolating and stigmatising the 'deviant' group which, in turn, leads to its alienation and isolation. They therefore turn to each other for support, share information, and engage in a renewed and escalated round of deviant behaviour, confirming the stereotypes. Nevertheless, Cohen accepts that, just because a person is labelled, this does not mean he necessarily accepts the label and behaves accordingly (Cohen 2002: 5). This is, perhaps, one reason why some moral panics 'fail' or, in other words, never amount to a true moral panic.

Deviancy amplification can also found in a more literal sense in the phenomenon of net-widening, whereby otherwise innocent people and innocuous activities peripheral to the core deviance are drawn into the definition and likewise labelled suspicious and deviant. In his Introduction to the 3rd Edition of his book, Cohen revised his view of deviancy amplification by rooting it more firmly in the constructionist perspective. He referred to:

> ...the thin idea of media-induced deviancy amplification. This is not causation in the constructionist sense - moral panics 'cause' folk devils by labelling more actions and

> people - but causation in the positivist sense and without the inverted commas. This psychology still uses concepts such as triggering off, contagion and suggestibility. Later cognitive models are far more plausible. For those who define and those who are defined, sensitization becomes a matter of cognitive framing and moral thresholds. Rather than a stimulus (media message) and response (audience behaviour) we look for the points at which moral awareness is raised ('defining deviance up') or lowered ('defining deviance down'). (Cohen 2002: xxiv)

This admits of the possibility that deviance amplification can be attributed to more zealous prosecution of offences which had previously been ignored, as Jenkins (1998) suggests. Heightened awareness may lead to diffusion, escalation and innovation in the societal control culture which in turn lead to a *seeming* increase in the incidence and frequency of deviance of a particular sort. In other words, the behaviour may have existed in those quantities before, but sensitisation has led to more of this behaviour being officially identified and brought to public attention.

The processes at work in the societal control culture are important. When a society perceives that it is under threat, one natural reaction is to strengthen the control culture in both formal and informal ways. The obvious formal institutions of the control culture are the police, the courts and the legislature. In the context of cyberterrorism, the intelligence agencies are also relevant because of the nature of the threat and its implications for national security.

During a moral panic, Cohen identified three processes at work at the formal level. First diffusion is found when the control culture gradually spreads out from the immediate vicinity of the original impact (Cohen 2002: 66). Ties between local and regional police forces are established and strengthened, and those between local and national levels of law enforcement (police, intelligence agencies, courts, legislature, Home Office) are activated in order to deal more effectively with the 'threat'. Second, escalation in the control culture may occur where the number of control agents is increased, and the scope and intensity of the control culture are extended. Third, innovation is found when new laws or new methods of applying existing laws are suggested and used. Innovation may exist at a number of levels: the police may become more proactive in enforcing laws they had hitherto not considered a priority; courts may extend or reinvent the application of existing law and increase the severity of sentences; governments may promulgate new law and order policies; and legislatures may pass new law. Such measures are justified by reference to the perceived threat and the generalised belief system which surrounds the threat (Goode and Ben-Yehuda 1994: 26-7; Cohen 2002: 66-7)

Despite Cohen's insistence on the need for a 'circular and amplifying' model (Cohen 2002: 13), his model of an individual moral panic, once distilled, is somewhat linear even if the social processes involved are indeed circular and amplifying (Critcher 2003: 13). The following model is constructed by Critcher out of the three elements described above – Cohen's classic statement, the disaster analogy and the deviancy amplification model – and modified according to Critcher's own findings in his meta-study of a series of moral panics to which Cohen's original model was applied (Critcher 2003: 151-4).

3.1 Emergence

Although the first element of the processual model concerns emergence of a moral panic, paradoxically, it is at this stage it becomes obvious that the model's value lies in its use as an heuristic device. It has no predictive value: emergence of a moral panic can only be ascertained retrospectively. There is not necessarily a key event which precipitates a moral panic. The perception of the threat, general apprehension and specific focus on imminent danger may emerge gradually. If there is a key event, it may happen during the moral panic rather than at the beginning and its importance is in what the event comes to symbolise as much as anything else. The researcher must look for the form in which the problem emerges, what is perceived as novel and how it is seen to threaten the moral or social order. Although a folk devil may be identified, this is not essential for a moral panic.

3.2 Media inventory

Here, the threat is explained and those responsible identified, primarily by way of the mass media who become sensitised to what has been identified as a social problem. Cohen identifies several processes at work: exaggeration/distortion, prediction and symbolisation. Stereotypes of who or what is responsible can be identified. Critcher argues that researchers should distinguish between different media constituents, so that sensitisation, exaggeration/distortion, prediction, symbolisation and stereotyping can be identified not just in the mid- and downmarket press, but also in the upmarket press and broadcasting.

Caution is required when identifying the rôle of the media in a moral panic. Media views should not be confounded with public opinion. Public opinion may follow that expressed in the media, albeit in an attenuated form (Cohen 2002: 49), however, it is not necessary for there to be strong public opinion on an issue for it to escalate into a moral panic (see further Section 4.1). Nor is the rôle of the media as simple as reporting the views of others. Cohen identifies three rôles, one or more of which the media may be

fulfilling in any given moral panic (Cohen 2002: xxiii). The first is agenda setting: the filtering of newsworthy events and the further refinement of choosing which issues to escalate and which to attenuate. The second rôle is image transmission. The media transmit the claims of claims-makers, again either enhancing or attenuating the rhetoric of moral panics. The third rôle of the media is that of claims-maker. Here, the media themselves are initiators, or at least organisers, of moral concern. Cohen has noted that the opinions portrayed by the media will not be homogeneous, and may be more extreme and stereotypical than opinions held by the public at large (Cohen 2002: 49).

3.3 Moral entrepreneurs/claims-makers

Groups or individuals can be identified as moral entrepreneurs, alternatively 'claims-makers', which may be more specific and a more accurate term. They may either lead, follow or operate in parallel with the media and will offer emotional and intellectual perspectives on the 'problem', generate images of the deviants and/or their behaviour and tender causal explanations. Some such groups may proffer what is best termed propaganda and stand ready to capitalise when a significant event occurs.

3.4 Experts

Experts are not straightforwardly distinguished from claims-makers. The researcher must identify who, if anyone, claims expertise and on what grounds, and whether they are accredited as experts by the media. Critcher notes that experts are often not prominent in a moral panic, indeed those claiming expertise are sometimes suppressed by the media. He finds it is much more common for claims-makers to be accredited as experts in order to lend greater weight to their claims, so that expertise is not so much inherent as bestowed by the media and political élites.

3.5 Elite consensus and concern, lack of organised opposition

This element is not present in Cohen, but was added by Critcher as a result of lessons learned from Goode and Ben-Yehuda (1994). A successful moral panic requires sufficient consensus and concern amongst élite groups, usually achieved through distortion of the issue. Distortion may be evident in disproportionality of the response when compared with either the objective severity of the condition or its causes and effects.

Élite consensus and concern can dominate, however, only when identified folk devils are vulnerable to attack, unable to fight back effectively and there is no-one else willing or able to speak up for them. As Cohen says:

> ...manipulation of the appropriate symbols ... is made easier when the object of attack is both highly visible and structurally weak. (Cohen 2002: 167)

Examples of 'failed panics' may occur where folk devils have successfully fought back, usually through gaining a voice in the media.

3.6 Coping and resolution

The media, claims-makers and experts will have pronounced on solutions to the problem. Existing powers of social control will be exploited, perhaps in innovative ways. If these are found insufficient, legal reform may follow. It is necessary to identify which solutions are advocated and by whom; whether they are instigated and by whom; whether there is procedural or legal innovation; and, most importantly, whether reforms are effective or symbolic. Critcher notes that such reform invariably heralds closure of the moral panic narrative.

3.7 Fade away

The moral panic may end, but there is always the possibility that it will re-emerge. When and why concern ends and whether it does or might recur must be established. The researcher should also identify the subsequent status of the problem. The decline of a moral panic may be explained by the manner of its ending, so that it either loses impetus, is routinised into existing frameworks or may be renewed by subsequent events.

3.8 Legacy

A moral panic may leave no lingering effect or it may produce profound and lasting changes in social policy, law or society's self-perception or identity. The latter may be evidenced by subtle shifts in the underlying social discourse, for example, the shift from youth to childhood described in Section 2.3. It is also important to establish the relationship of a moral panic to previous and subsequent events.

4. GOODE & BEN-YEHUDA: THE ATTRIBUTIONAL MODEL

The contextual constructionist perspective is crucial to an understanding of the work of Goode and Ben-Yehuda (1994). They assert that, although the relationship between the social construction of a problem and its objective nature may be problematic, nevertheless, it is still capable of empirical verification.

> The moral panic is a phenomenon - given its broad and sprawling nature - that can be located and measured in a fairly unbiased fashion. It does not matter whether we sympathize with the concern or not. What is important is that the concern locates a "folk devil", is shared, is out of synch with the measurable seriousness of the condition that generates it, and varies in intensity over time. ... The point that the moral panics concept is scientifically defensible, and not an invidious, ideologically motivated term

> of debunking, needs to be stressed in the strongest possible fashion. (Goode and Ben-Yehuda 1994: 41)

The point made in Section 2.1 above, that measurement of concern against seriousness (disproportionality, put another way) is not an unproblematic concept, applies equally here. Goode & Ben-Yehuda assert that measurement can be reasonably unbiased, yet there is always the issue of the researcher's position in the research. It is the importance of the interpretation of the researcher in moral panic research which gives rise to the criticism of ideological motivation.

Goode & Ben-Yehuda's model, deemed the 'attributional model' by Critcher (Critcher 2003: 23), is made up of five elements: concern, consensus, hostility, disproportionality and volatility (Goode and Ben-Yehuda 1994: 33-41).

4.1 Concern

Moral panic involves heightened concern about a certain issue which is manifested in measurable ways. Goode and Ben-Yehuda specify the use of "opinion polls, public commentary in the form of media attention, proposed legislation, social movement activity, and so on" (Goode and Ben-Yehuda 1994: 33). However, empirical evidence of *public* concern is one of the most problematic elements of the attributional model, and some researchers have fudged this issue by equating public concern with media reaction and/or legislative activity (Ungar 2001). This is unsatisfactory. Public opinion may follow media coverage, albeit in an attenuated form (Cohen 2002: 49). Yet at other times the media invoke or construct public opinion in order to add weight to a narrative and Critcher therefore concludes that public opinion should be considered one of the unnecessary factors in the attributional model (Critcher 2003: 150).

It is, however, crucial to a moral panic that claims-making activity leads to concern among the political and media élites. The task is to assess the concern here and understand how and why these social forces become convinced of the gravity of a given problem.

4.2 Hostility

Goode & Ben-Yehuda saw folk devils, constructed through a process of stereotyping, as essential to a moral panic (Goode and Ben-Yehuda 1994: 33). Increased levels of hostility are displayed towards those identified as folk devils and as engaging in behaviour perceived as threatening to the values, interests or existence of society, or a segment of it. They are characterised unambiguously as the 'enemy', harmful and threatening.

Critcher has found that a successful moral panic does not necessarily require a folk devil, and it would be a 'serious empirical mistake' to assume otherwise (Critcher 2003: 150). Nevertheless, in the case of cyberterrorism, it happens that two classes of folk devil are easily identified: the hacker and the terrorist.

4.3 Consensus

There is no rule as to how many people make a moral panic. It is not necessary for every member, nor even a majority, of the society to experience concern or partake in the consensus.

> ...moral panics come in different sizes – some gripping the vast majority of the members of a given society at a given time, others creating concern only among certain of its groups or categories...Consensus that a problem exists and should be dealt with can grip the residents of a given group or community, but may be lacking in the society as a whole; this does not mean that a moral panic does not exist, only that there is group or regional variation in the eruption of moral panics. (Goode and Ben-Yehuda 1994: 34).

At some point in a moral panic, concern condenses into a consensus about what the threat is, who is responsible for it, and what the solution should be. Consensus need not be universal and is a matter of degree. However, in a moral panic, there is an unusually high level of consensus in society or the relevant segment of society (Goode and Ben-Yehuda 1994: 102). On the other hand, consensus may be prevented and the panic made to fail by organised opposition to the claims-makers. Claims are often contested in a moral panic, but the extent to which these counter-claims are heard depends on which messages the media amplify and which they attenuate.

Once again, there are empirical problems in locating the wider consensus in society. More important, and essential to a successful moral panic, is the identification of a consensus among élite elements across pressure groups, media and politicians. Any model of moral panic should retain the insight that the "extent and nature of opposition within élite opinion is an important determinant of the outcome of a potential moral panic" (Critcher 2003: 151).

4.4 Disproportionality

Notwithstanding the critique discussed above (section 2.1), the concept of disproportionality is fundamental to moral panic and it is evident when fear and concern exceed the levels which are deemed appropriate and directly proportionate to the objective nature of the threat.

> ...certain fears and concerns must be grounded in the conditions of social and economic life; they do not arise for no reason at all. At the same time, these concerns *may* be

> fuelled by specific threats that are materially nonexistent or grossly exaggerated. (Goode and Ben-Yehuda 1994: 49)

Goode and Ben-Yehuda identify four indicators of disproportionality (1994: 43-5):

1. statistics have been exaggerated;
2. statistics have been fabricated;
3. the attention paid to condition A is vastly more than the attention paid to condition B, where B is as harmful or more so than A; or
4. the attention paid to condition A at time X is vastly more than the attention paid at an earlier or later time Y where there is no change in the objective seriousness of condition A between times X and Y.

Critcher has noted that exaggeration of the magnitude of the social problem is extremely important but so, too, is the distortion of its causes and effects (Critcher 2003: 151). The element of disproportionality should, therefore, be considered to be wider than simple exaggeration and should include these different kinds of distortion.

4.5 Volatility

The element of volatility is the logical adjunct to the concept of panic. A panic erupts suddenly and dramatically, and then subsides. Volatility essentially refers to the fluctuations in levels of social concern over a particular issue, here one day and gone the next.

Of the criticisms levelled at moral panic, two are related: criticisms of the use of the term 'panic' and of the notion of volatility. Cohen has noted the pejorative connotations of the term 'panic' which is associated with irrationality, lack of control and baying mobs. He considers these connotations unfortunate and has accepted "the downgrade of 'panic' to a mere metaphor" (Cohen 2002: xxvii). Nevertheless, he stands by the analogy, arguing that recent literature on disasters, both natural and man-made, has emphasised the social element in these episodes (eg Scraton 1999). The related criticism of the concept of moral panic is that relating to volatility (Thompson 1998: 8-11; McRobbie and Thornton 1995). It is argued that volatility of concern in society has actually given way to a permanent sense of unease, so that panics are no longer discrete, but more sequential or continuous and simply move from one area of anxiety to another. McRobbie and Thornton have argued that relations between social groups and the media, 'reality' and representation are now so complex that even an updated model of moral panic cannot take account of these complexities. The concept of moral panic as a

genuine social phenomenon is outdated and, far from being volatile episodes, have become:

> ...a standard response, a familiar, sometimes weary, even ridiculous rhetoric rather than an exceptional emergency intervention. Used by politicians to orchestrate consent, by business to promote sales ... and by the media to make home and social affairs newsworthy, moral panics are constructed on a daily basis. (McRobbie and Thornton 1995)

In so far as the claim is that there are more panics occurring in recent years, this does not necessarily negate the element of volatility. If the claim is that we are, somehow, in a 'permanent moral panic', then this is an oxymoron: by definition, a panic is temporary (Cohen 2002: xxix). Nevertheless, its temporary status may last months or even years. Panics may also be sequential, the subsequent panic building on the previous one and continuing the narrative. Periods of greater intensity can often be identified at different times during longer episodes. In short, the criterion of volatility can be expressed in myriad ways and this vagueness makes it one of the least useful and testable attributes of a moral panic. In consequence, Critcher recommends that it be abandoned (Critcher 2003: 151).

Volatility is, however, the element most closely linked with historical context. It goes to the heart of essential and under-researched questions, such as 'why do moral panics start?'; 'why do some potential panics fail?'; and 'why do moral panics end?'. If we are to avoid a positivistic, formulaic, cyclical approach to the study of moral panics by emphasising historical context, answers to these questions are essential, although perhaps not under the, too general, rubric of 'volatility'.

4.6 Claims-makers

Critcher adds this sixth attribute to the original list of five because claims-makers are fundamental to the constructionist perspective espoused by Goode and Ben-Yehuda. The rôle of claims-makers is central to the cultural and political struggles over social problem definition and they may be of one of two types: rule creators, who seek to impose their morality and beliefs on others; and rule enforcers, who are less ideologically motivated and more concerned with promoting the business of rule enforcement. Claims-makers may, therefore, operate for ideological or economic reasons. This is characterised as exploitation, which uses the mechanisms of deviance amplification and orchestrating social reactions to achieve social control. According to Ungar (2001), this social manipulation leads to the desired state of panic, having a consolidating influence on consensus, which rallies to the dominant ideology.

The researcher should identify: who the claims-makers are; whether relevant organisations are already in existence or are formed in response to the specific social problem; what strategies are adopted for claims-making; and whether the media themselves are engaging in active claims-making (Critcher 2003: 151).

5. MORAL PANIC AND CYBERTERRORISM

It was amply demonstrated in Chapter 2 that the technical definition of cyberterrorism is contested. Yet cyberterrorism is more than just a technical act, it is also the term applied, in a wider social context, when fears about the intersection of terrorism, technology and hacking rise to the surface. This study characterises cyberterrorism as a socially constructed phenomenon, widely discussed in society as if it is a current problem yet, with the caveat that the government and security services may be in possession of classified information relating to cyberterrorist activity, a genuine cyberterrorist attack has never been publicly identified. The focus of this study is, indeed, the social construction of cyberterrorism and not the likelihood or otherwise of its occurrence. As Cohen argues:

> The idea that social problems are socially constructed does not question their existence nor dismiss issues of causation, prevention and control. It draws attention to a meta debate about what sort of acknowledgement the problem receives and merits. The issue indeed is *proportionality*. (Cohen 2002: xxxiv)

This is exactly the point with reference to cyberterrorism. Only in deconstructing the social construction can we arrive at an understanding of the status quo and navigate to a solution, although the latter is outwith the scope of this study. Moral panic remains a sharp sociological tool where an issue 'emerges as a symbolic threat' (Critcher 2003: 154). When viewed as an heuristic device, it is clear that it can be used to expose definitions of cyberterrorism; who is constructing them and who is contesting them; the extent to which these definitions are accepted by media and political élites; the rôle of experts in defining the problem and constructing the solution; and how the state is dealing with the issue in terms both of claims-making and instituting repressive measures by way of a 'solution'.

There are other ways of excavating the social construction of cyberterrorism. It is arguable that there is no need for an established analytical or theoretical framework in order to conduct this study with rigour. Grounded theory methods, addressed in detail in the following chapter, might on their own be used to identify emergent concepts, categories and relationships from the chosen corpus of data and integrate them into a substantive theory which explains what is going on in the particular case of

cyberterrorism. As it turns out, grounded theory methods are indeed important to this study, but it was felt that the moral panic framework – particularly the use of both models at different stages of this study – would be valuable for comparison with the emergent findings of this study and that these findings might, in turn, add something to the moral panic literature. At the very least, moral panic provides a context for the discussion of the findings on the social construction of cyberterrorism.

An alternative approach to moral panic can be found in the Social Amplification of Risk Framework (Kasperson, Kasperson et al. 2003), which is increasingly popular within the Information Systems domain. SARF considers how risk communication interacts with social, psychological, institutional and cultural processes to produce interpretations of risk. Clearly there are close parallels with deviance definition here. Risks may either be amplified, as in a classic moral panic, or attenuated, as in a failed panic. However, the overall framework is based on a classic, linear communication model, despite the feedback and iteration apparent in the amplification and attenuation phases. This leads to a tendency towards a 'ticking the box' approach when fitting a given social phenomenon inside the framework and historical context may be underplayed. Moreover, SARF is primarily concerned with risk, whereas moral panic places greater importance on morality, which is such an essential part of the pervasive terrorism narrative of 'good' and 'evil'. Perception and acceptance of risk is so often tied to a process of blaming, the obvious moral dimension of which is better highlighted by moral panic. An account of moral panic will place the media in a central rôle, yet SARF views it as a stage in the linear process, a conduit for, rather than originator of, information. There is also an emphasis on public perception, whereas moral panic admits of the possibility that amplification of social problems need only occur at the élite levels of society for far-reaching social consequences to ensue. For these and other reasons, moral panic was considered a better framework for the study of cyberterrorism giving, as it does, a more rounded view of socio-political processes and a stronger emphasis on morality. SARF's emphasis on the public perception of risk will undoubtedly be important in future studies in this area, but it was not the intention in this study to put that issue centre-stage.

Both the attributional and processual models of moral panic described in this chapter will be used to frame this study and their precise rôle is discussed in the following chapter.

CHAPTER 4

METHODOLOGY AND RESEARCH DESIGN

1. METHODOLOGY

It is apparent from the review in Chapter 2 that social science studies of cyberterrorism from an interpretative perspective are almost entirely absent from the literature. This study is an attempt to step into that gap. Whereas the emphasis in the existing literature is often on description and prediction of cyberterrorist behaviour which then form a basis for proposed solutions, this study seeks to understand the phenomenon of cyberterrorism as a process of social definition. The research approach follows the interpretivist tradition which eschews the notion of a single, objective reality and emphasises the existence of many differing perspectives on the same reality (Walsham 1993). Social constructions such as language, consciousness, shared meanings, documents, tools and other artefacts are considered to be the source of knowledge of reality (Klein and Myers 1999) and there is a focus on complexity in the way humans make sense of the world and on the communicative properties of all social processes (Kincaid 1996). Orlikowski and Baroudi give a detailed account of interpretative research in the IS domain (1991). Ontologically, social reality is not given, but can only be interpreted:

> [I]nterpretive researchers recognize that as meanings are formed, transferred, and used, they are also negotiated, and hence that interpretation of reality may shift over time as circumstances, objectives, and constituencies change. (Orlikowski and Baroudi 1991)

Epistemologically, social processes can only be understood from the point of view of those engaging in them, so that the language humans use to describe those processes is key.

> Understanding social reality requires understanding how practices and meanings are formed and informed by the language and tacit norms shared by humans working towards some shared goal. (Orlikowski and Baroudi 1991)

The task of the interpretative researcher, according to Orlikowski and Baroudi, is to explain how these subjective meanings are created and maintained in a particular social context. However, the researcher cannot assume a neutral position in relation to his investigation, which is inevitably shaped by his own assumptions, beliefs, values and

interests. A 'strong' constructionist view considers the researcher to be inextricably a part of his account of a social phenomenon and is presumed to enact the social reality he is studying (Astley 1985; Orlikowski and Baroudi 1991). He has no access to reality except through his own knowledge and experiences. On the other hand, on the 'weak' constructionist view espoused in this study, the researcher attempts an understanding of meaning systems shared by actors by means of an interpretation of the data he has collected and an account of what these actors are doing, how and why (Fay 1987). A high degree of reflexivity is required if he is not to skew his account of the object of study.

Klein and Myers' account (1999) of interpretative research within the IS domain was particularly influential when trying to enhance the opportunities for reflexivity during the design phase of this study. They distinguish a set of seven principles for the construction and evaluation of field research in the interpretive paradigm from the philosophical perspective of hermeneutics. The authors argue that the "emergent nature" of interpretivist research is not necessarily compromised by a set of principles, so long as the researcher uses them as a means to exercise judgment and avoids slavish adherence. Use of these principles makes explicit that all angles have been considered by the researcher and provides an evaluative tool by which others may judge the work. The seven principles, although originally conceived for application to field studies, are particularly relevant to this study, since the model of moral panic was chosen first, and the subsequent process of textual data collection and analysis had to be divorced from the model. Only on this basis could there be a meaningful discussion of how the findings compared with the 'ideal type' moral panic described by the model. The principles and their application to this study are, in summary, as follows:

1. The fundamental *principle of the hermeneutic circle*, "a meta principle on which the following six principles expand". Human understanding is achieved through iteration between understanding of the meaning of inter-dependent parts and understanding of the whole. The iterative nature of the analytic process used in this study will be made apparent below and this fits very neatly with the principle of the hermeneutic circle.

2. The *principle of contextualisation* requires the author to pay particular attention to the social and historical background of the research setting. There is an inevitable difference in understanding between the researcher and the author of a text, created by the historical distance between them. People are both products and producers of

history. Moral panic researchers must constantly ensure that their research is grounded in its social and historical context in order to understand the social definition of and reaction to social problems and to avoid recourse to positivist views of historical cycles.

3. The *principle of interaction between the researcher and the subject*. The researcher must acknowledge his interaction with the subject of study. This is most important in studies involving personal interaction between researcher and participant, such as field studies. However, the principle has relevance in studies like this which use textual analysis because the researcher must have a critical awareness of how his construction of a corpus of data will affect the results of the study.

4. The *principle of abstraction and generalization.* Whilst not theory-testing in any positivist sense, it is possible to relate the particular details discovered to wider propositions which describe the nature of human understanding and social action. This is precisely the process involved in comparing the evolution of social processes with an 'ideal type' such as moral panic.

5. The *principle of dialogical reasoning.* In hermeneutics, prejudice is seen as a necessary starting point for understanding. The researcher must confront his preconceptions (prejudices) which guided the original research design with the data which emerge. This is a repeated and iterative process. Philosophical assumptions must be made explicit. When coding the corpus of data in this study, it was necessary to start with an idea of what to look out for based on assumptions derived from moral panic. These ideas changed constantly and were frequently revisited during the coding process so that preconceptions which did not stand up to the data were modified or abandoned.

6. The *principle of multiple interpretations* requires the researcher to seek out, examine and explain possible differing interpretations among actors which may, for example, be expressed in multiple narratives. "Even if eventually none are found, the principle of multiple interpretations is of heuristic value because it leads to probing beneath the surface." Multiple interpretations, and their eventual distillation into a consensus, are central to the social processes evident in a moral panic. This principle is, therefore, extremely important.

7. The *principle of suspicion*, which is used more in critical social theory than interpretivism. The idea is not to take things at face value and to reveal socially

constructed distortions and delusions. An ideal type moral panic is based on distorted claims and these must first be recognised, then their genesis and effects explained. This principle highlights the fact that, although moral panic research can be carried out within the interpretivist tradition, there are elements which nod towards critical social theory, particularly the debunking of myths and the idea that clarity of understanding will unveil vested interests and empower people to engage in social change.

Making explicit the interpretative perspective of this study is particularly important because it is possible to use the moral panic model in a linear and deterministic fashion which would correspond more to a positivist approach to theory testing. Indeed, Cohen has been accused of ignoring historical context and claiming that the cycle of a moral panic is historically timeless (Hunt 1997). This problem is overcome if it is made explicit that the model is used as an heuristic device, as Critcher suggests (2003: 2), which allows the researcher first to identify patterns in a narrative and only then to compare those patterns against the ideal type of a moral panic. Although there may be a meta-structure for all moral panics which would include some or all of the elements outlined in the processual and attributional models, the particular route which the panic takes and the way it is expressed by different sections of society will be different in each case. This is why the use of moral panic as an heuristic device rather than as a diagnostic tool is important.

In order to operationalise this strategy, it was necessary to provide a link between the corpus of data used and the moral panic model. Moreover, the research method used had to be grounded in the corpus so that any patterns identified could truly be said to have been derived from the corpus rather than imposed by the moral panic framework. Two possible approaches which were considered were Critical Discourse Analysis (CDA) and content analysis. CDA is relevant to this field of study in that it is fundamentally concerned with the investigation, from a critical perspective, of "social inequality as it is expressed, signalled, constituted, legitimized and so on by language use (or in discourse)" (Wodak 2001). Discourse is considered both as an instrument of power and control and as an instrument of the social construction of reality (van Leeuwen 1993). CDA researchers see ideology as instrumental in the maintenance of unequal power relations and one of the central aims of CDA is to demystify discourses by deciphering these ideologies (Wodak 2001). CDA focuses not only on texts, but also

on the social processes and structures which give rise to the production of those texts and how individuals and groups give those texts meaning.

This fits with moral panic which is, in part, concerned with power inequalities in the processes of social definition, resulting in a deviant class being defined and cast outside "acceptable" society. Moral panic research is traditionally carried out using a variety of texts, often drawn from the mass media, and it is easy to see how CDA could be used as the linking mechanism between data and the moral panic framework. Meyer (2001) has noted that it is permissible to use CDA in conjunction with a wide variety of theories and frameworks, and moral panic would be no exception. Moreover, Meyer states that the processes of data collection and analysis are not considered discrete, so that the two may go along together, stepwise, until an acceptable degree of saturation is reached. Accordingly, CDA methodology is often placed in the hermeneutic tradition.

A wide variety of methodologies can be found within the realm of CDA, including those dealing with mass media coverage and large data corpora like the one in this study. However, despite the wide field of application of CDA, this tradition represents a step too far for the purposes of the research aims of this study. The major reason for this is the fact that CDA has its roots in, and is fundamentally concerned with, linguistics. Meyer is quite specific that "in contrast to other approaches to text and discourse analysis (for example, content analysis, grounded theory, conversation analysis...) CDA strongly relies on linguistic concepts such as actors, mode, time, tense, argumentation and so on" (Meyer 2001). The study presented here does not go this far. The core operationalisations of this research are topics and contents, not linguistic concepts. Put another way, this study is a first step in demystifying a topic and its related concepts. A next logical step would be to go further and examine the language used in the context of a true discourse analysis using CDA. This study does not set out to achieve an analysis of the discourses involved in cyberterrorism: it merely identifies those discourses as being present and in need of further research.

Content analysis (CA) is another methodology which might have been chosen for this study. CA was developed for social research as a method for analysing textual materials, specifically newsprint. It is a very general approach, is able to deal with large quantities of data and lends itself particularly to historical data. Bauer (2000) presents it as a systematic, procedurally explicit and replicable technique for making inferences from a text to its social context. He notes that a given text may allow the researcher to draw inferences about the "worldviews, values, attitudes, opinions, prejudices and

stereotypes" of the source of the text. Equally, each text has an audience in respect of whom the text is a "medium of appeal" which may have an "influence on people's prejudices, opinions, attitudes and stereotypes". CA has, for example, been used in media-effect studies on agenda-setting (Neumann 1989). However, the fact that CA often involves statistical treatment of texts gives the clue that it is most often used in positivist qualitative research and is, therefore, not ideal if the researcher wishes to take an interpretative approach, as in this study. Although the method is flexible enough to accommodate a wide range of theories and research problems, the rigid nature of the coding frame is too inflexible for the purposes of this research since it is constructed in advance, albeit with reference to the texts themselves, and then imposed on the texts. A more flexible approach was required, one which evolved out of the texts themselves on an ongoing basis and could take account of rarity and absence, as well as presence, of a concept. This is why Grounded theory was considered the most appropriate method.

In *The Discovery of Grounded Theory*, Glaser and Strauss (1967) presented a method consisting essentially of systematic, inductive guidelines for collecting and analysing data with the ultimate goal of building substantive theories explaining the collected data. Although a considerable variety of grounded theory approaches has developed over the last 40 years, a number of strategies can be identified which are common to most: simultaneous collection and analysis of data; a multi-stage coding process; comparative methods; memo writing aimed at the construction of conceptual analyses; theoretical sampling to refine emerging ideas; and integration of the theoretical framework (Charmaz 2000).

As Grounded theory became more popular and was elaborated, Glaser and Strauss began to part ways, a development which became most apparent with the publication of Strauss and Corbin's book *Basics of Qualitative Research: Grounded Theory Procedures and Techniques* (1990) to which Glaser made a critical reply (Glaser 1992). Strauss and Corbin later updated their work in a second edition (Strauss and Corbin 1998). In essence, Strauss and Corbin's work elaborated a series of analytic steps, provided detailed examples and introduced new techniques. Although the second edition was less prescriptive, Glaser (1992) considered their developments to be made at the expense of the emergent and open-ended character of Glaser and Strauss' earlier work. Strauss and Corbin emphasised the qualities of validity, reliability and verification, whereas Glaser emphasised the emergence of theory through the analysis of basic social processes using constant comparison. Glaser (1992) considered that

Strauss and Corbin were forcing data and analysis through their preconceptions, questions and techniques and argued that constant comparison should be sufficient. He asserted that the purpose of grounded theory methods should be to generate theory, not to verify it through a method which really amounts to full conceptual description rather than theory building. Nevertheless, Strauss and Corbin's statement of the significance of description and conceptual ordering for theory development is compelling (Strauss and Corbin 1998: 16-21) and there is no doubt that their methods are aimed at theory building, albeit not with the same purist zeal that Glaser espouses.

Strauss and Corbin's 1998 edition of *Basics of Qualitative Research* was chosen as the guiding text for this study precisely because they offer a rich variety of strategies for conceptualising, ordering and theorising about data. Although the Glaser critique suggests that their prescriptions risk the forcing of data into a framework, Strauss and Corbin are not necessarily as prescriptive as all that. As Charmaz points out (2000), readers may reify authors' earlier written words and this may account for the view that they have presented a method to be unswervingly followed. Strauss and Corbin demonstrate more flexibility in their approach to theory building than Glaser gives them credit for and allow that grounded theory may be used for other purposes:

> We also believe that we have something to offer in the way of techniques and procedures to those researchers who want to do qualitative analysis but who do not wish to build theory. Building theory is not the only goal of doing research. High-level description and what we call *conceptual ordering* also are important to the generation of knowledge and can make a valuable contribution to a discipline. (Strauss and Corbin 1998: x)

In this study, the central concern is to understand how cyberterrorism has been constructed and the representation of this issue in the UK national press has been chosen as the most effective and efficient focus for the study. The use of moral panic as an heuristic device, a framework against which the case of cyberterrorism might be compared, gives a clear direction to the study but this does not mean that it should drive the data analysis. To the contrary, the analysis has to be explicitly divorced from the details of the moral panic framework in order for the comparison between the patterns emerging from the data and the moral panic framework to have validity. The insistence of grounded theory methodology on the emergent quality of theory from data is the principal reason for choosing this approach. This research does not set out to prove or disprove a hypothesis that the social reaction to cyberterrorism amounts to a moral panic. Rather, it seeks to describe the social processes which appear to be at work, to formulate an explanation of what is going on ("substantive theory building" in the sense

meant by Strauss and Corbin) and to compare this explanation to the moral panic model. The approach set out by Strauss and Corbin (1998: eg 49, 80, 155) admits of the use of their grounded theory methods for these purposes. As well as providing a theoretical explanation of the social processes at work in the particular case of the social construction of cyberterrorism, the findings of this study will also contribute to the wider debate on moral panic by adding another case to the literature, discussing the relevance and usefulness of the moral panic framework and making some modest suggestions for modification.

2. RESEARCH DESIGN

2.1 Summary

The aim of this study is to explore how cyberterrorism has been socially constructed. Moral panic has been identified as a suitable heuristic device to enrich the analysis of the relevant social processes and two distinct models of moral panic, Cohen's processual model and Goode and Ben-Yehuda's attributional model, were summarised Chapter 3. The research design is, in essence, as follows. This is a study focussed on the UK. All available articles in the UK national press relevant to cyberterrorism were collected and their text imported into new project, called a 'hermeneutic unit', in Atlas/ti, a software application designed to assist grounded theory researchers. These texts were then coded extensively. Some codes were identified in advance with reference to some very general notions, derived from the literature, of what concepts might turn out to be relevant and were used from the start in order to generate some quantitative frequency data. The vast majority of the codes, however, were the result of an iterative, multi-stage coding process from which qualitative concepts emerged in accordance with grounded theory methods. An extensive approach was taken to the coding process and everything of relevance to the issue of cyberterrorism was coded, regardless of relevance to one or other of the moral panic models. The results are written up in Chapters 5-8 and organised according to the six elements of the attributional model of moral panic. A large amount of axial coding and theoretical sampling was carried out at the writing-up stage in order to effect a more nuanced analysis and build a more complete and balanced explanation of the social processes identified. Finally, the findings in relation to the social construction of cyberterrorism are discussed in Chapter 9 and these findings are compared with the framework provided by the processual model of moral panic. The subsidiary question whether cyberterrorism amounts to a moral panic is answered. The use of the grounded theory

methods, together with the deployment of two distinct models of moral panic at different stages of the research process, enabled a rich picture of the social construction of cyberterrorism is built up.

The following account of the research process is inevitably artificial, since it splits the discussion into distinct stages of corpus collection and analysis. In reality, these two activities occurred more or less simultaneously and carried on well into the writing up phase. This approach is dictated by grounded theory methods which can, in this sense, be characterised as being within the hermeneutic tradition. Nevertheless, in the interests of clarity, it is convenient to consider corpus collection and analysis separately for the purposes of the following explanation

2.2 Corpus collection

The grounded theory methods of Strauss and Corbin do not have much to say about the choice of a research question and the initial location of data sources, beyond setting out a number of practical considerations (Strauss and Corbin 1998: 29-34, Chapter 4). It is really up to the researcher to decide where and how to start collecting data, with subsequent data collection being driven by the analysis itself. The concept of sampling and its associations with quantitative research and the positivist paradigm is inappropriate in this study. The concept of corpus construction, in this case referring to a corpus of data built up with reference to the principles of relevance and saturation, is more appropriate (Bauer and Aarts 2000). Construction of the corpus of data for this study had four distinct stages: first, the source of the data was chosen; second, relevant data were extracted by means of a carefully refined search string; third, the results were sifted for relevance and duplication; fourth, additional texts were added where, during the coding process, it became apparent that certain data were missing and needed to be incorporated. The processes involved are set out in more detail in the remainder of this Section.

It will be apparent from Chapter 3 that a study of moral panic might use data from a large number of sources. For example, Cohen's study on Mods and Rockers used sources including local and national press, radio and television broadcasts, parish newsletters, Hansard, correspondence received by a relevant pressure group and interviews with members of the public (Cohen 2002: 173). The disturbances Cohen investigated were limited in time – 1964-1966 – and space – a handful of English seaside resorts – and he was able to consider multiple sources without drowning in information. The list of potential sources of data relevant to the social construction of

cyberterrorism is, similarly, very broad and would include the national press, information security industry publications and research, police publications and statements, government publications and statements, political reports, public interviews, interviews with hackers and so forth. The concept of cyberterrorism, however, is at least 20 years old and the sheer volume of potentially relevant information is overwhelming. It is not possible, therefore, for one researcher to make sense of multiple sources of information in the time allowed for a PhD.

It was decided that the UK national press would be a sufficient and appropriate source of data for the study of the social construction of cyberterrorism. This can be justified by reference to the moral panic model, in which the media play the central rôle in bringing an issue into the public domain. Media sensitisation to a social problem puts it on the public stage; they report the claims of claims-makers and those who are not reported are excluded from the public discourse; they attribute expertise to those deemed worthy to pronounce on the problem and solutions; with politicians, they construct an élite consensus; and when they loose interest, the issue fades from public attention. In other words, anything which does not pass through the filter of the media is, by definition, excluded from the discourses which make up a moral panic. Absence is important, of course, and it was necessary to be aware of what was being excluded as well as what was included. The national press is, clearly, only one constituent of the media but it is an obvious choice for a study such as this where time and resources are not limitless and choice of data source is, for pragmatic reasons, dictated by ease of access and the lack of any need for transcription. The choice of data source inevitably affects the scope of the findings of this research because the claims of claims-makers can only be discussed to the extent that they have been reported in the UK national press and have inevitably passed through at least two interpretive filters: the journalist and the researcher. Such a study can say nothing about issues which have been neglected by the press but which may be considered important by other claims-makers. Nevertheless, it was decided that the findings, such as they might be, would still be interesting and there is always the possibility of taking the research into different areas in the future. In some respects, this is a penalty inevitably paid by a researcher entering a subject area not yet well-covered in the literature and the researcher must, accordingly, be content to take and give an account of those first steps.

The Lexis-Nexis Professional service was used as the most efficient, comprehensive and searchable source of UK national press articles. Nevertheless, Lexis-Nexis coverage is variable, and the details are set out below.

Publication	Days published	Date Lexis-Nexis coverage starts
The Guardian	Mon-Sun	14 July 1984
The Times	Mon-Sat	1 July 1985
Sunday Times	Sun	1 July 1985
The Independent	Mon-Sat	19 September 1988
Independent on Sunday	Mon-Sat	19 September 1988
The Observer	Sun	7 October 1990
Daily Mail	Mon-Sat	1 January 1992
Mail on Sunday	Sun	1 January 1992
The People	Sun	2 January 1994
Daily Mirror	Mon-Sat	29 May 1995
Sunday Mirror	Sun	29 May 1995
The News of the World	Sun	26 July 1998
The Business	Sun	2 May 1999
Sunday Business	Sun	2 May 1999
The Express	Mon-Sat	2 October 1999
Sunday Express	Sun	2 October 1999
The Sun	Mon-Sun	1 January 2000
The Daily Telegraph	Mon-Sat	30 October 2000
The Sunday Telegraph	Sun	30 October 2000
Daily Star	Mon-Sat	15 December 2000
Morning Star	Mon-Sat	2 July 2001
Sunday Star	Sun	15 September 2002

In order to generate the most complete corpus of data possible, searches were performed on the whole Lexis-Nexis database of UK national newspapers. No back-stop date was imposed and all dates were searched up to 31 December 2005. Collecting data from complete years was important for the purposes of quantitative analysis and this is why data from the available part of 2006 were not included. A search string was constructed to collect all articles referring to both hacking and terrorism in some form. Some of these articles refer to cyberterrorism specifically, but many do not: it was necessary to cast the net wide in order to gain a sense of how the portrayal of hackers and terrorists separately impacts on the portrayal of cyberterrorism specifically. Several preliminary search attempts were made and a high-level analysis of the results was performed. The results of this analysis were then used to refine the search string in order to exclude

irrelevant data and include data which was discovered to be relevant. The eventual form of the primary search string was:

(cyberterror! OR cyber-terror! OR cyber w/1 terror!) OR (information pre/1 terror!) OR ((hacker! OR hacking) AND terror!)

A number of problems had to be resolved in the course of defining this search string. Hack! is not a useful search term, since it throws up large volumes of articles using the word 'hack' to refer to journalists or politicians in the pejorative. Hackney, in London, also features prominently. To define such instances out of the search string is extremely difficult and hardly worth the effort due to the minimal number of relevant articles using the word 'hack' but not the more usual 'hacker' or 'hacking'. The term 'hacked' has similar problems. It can be used in the sense of 'hacked into a computer', but this is rare in the absence of the terms 'hacker' or 'hacking' in the same article. 'Hacked' is far more often used in the sense of 'hacked off', therefore it is left out of the search string. The search string 'information pre/1 terror!' was used in an attempt to capture references to 'information terrorism'. As it turns out, this term is not much used in the UK national press, 'cyberterrorism' being by far the more common term.

These results were then sifted for relevance and duplicates and the coding process was begun. As new concepts emerged from the coding of the data and the making of comparisons between these concepts, gaps in the data were discovered and variety in the data hinted at, indicating that a fresh round of data gathering was necessary in order to maximise the opportunities to document variations between concepts and to add properties and dimensions to the emergent code categories. This is what Strauss and Corbin term theoretical sampling (1998: Chapter 13), although the use of this technique was relatively limited due to the very wide net cast for the original corpus of data. For example, during the sifting and coding processes, variety in the terms used to denote cyberterrorists was discovered in the texts, such as 'techno-terrorists', 'electronic terrorists', 'e-terrorists' and 'IT terrorists'. These terms were made the subject of a new Lexis-Nexis search and the results sifted again. The results of this type of sampling were not always fruitful. 'IT terror!' did not produce any useable results since Lexis-Nexis considers invisible such small words as 'it', 'the', 'all' etc. Thus a search for the specific term 'IT terror!' threw up results such as "It was the terrorists...". When sifting through around 270 results on an all-dates search, no instances of the use of the term 'IT terrorism' or its variants were found.

The corpus resulting from this extended collection process comprises 681 articles, the first of which is dated 26 May 1987 and the last 31 December 2005. Each relevant article was saved as a separate .txt file with a file name identifying the date and name of publication.

2.3 Corpus analysis

To facilitate the analysis of the corpus, each article in .txt form was loaded as a 'primary document' into a new 'hermeneutic unit' in Atlas/ti, a software programme designed to assist qualitative researchers, particularly those using grounded theory methods. Such software is no substitute for the researcher's understanding of the meaning of texts, but it does assist with a large number of, sometimes quite complex, mechanical tasks (Kelle 2000). Using grounded theory methods, data analysis and theory construction are closely linked and it is necessary to keep track of the various concepts, ideas and arguments which the researcher generates during the course of the analysis. This is often a mammoth task and so it proved to be the case with this study: analysis of the collected texts took a little over 18 months.

Atlas/ti facilitates many of the techniques described by Strauss and Corbin, including open, axial and selective coding, the creation and ordering of memos and diagrams and, perhaps most importantly of all, a sophisticated mechanism for retrieving coded segments of texts. In Atlas/ti, the retrieval mechanism can be used to build 'queries' which allow the researcher to compile, for example, a Boolean search combining a variety of different concepts and categories in order to retrieve very specific items from a large body of data. More information on the use of Atlas/ti in this study is presented in the Appendix.

(a) Quantitative data

It is possible to refine Atlas/ti techniques to elicit quantitative, as well as qualitative, data. These techniques are not necessarily made explicit by the authors of Atlas/ti (www.atlasti.com/manual.html) but the software is sophisticated enough that, if the researcher finds he or she needs to achieve a certain result, it is nearly always possible to identify a work-around which will do the job. A combination of coding, categorisation and retrieval mechanisms was used to compile some sophisticated quantitative data which are presented in Chapters 5-8.

Despite a tendency to associate quantitative data with positivist research, there is no reason why quantitative data should not feature in an interpretative study and there is a

current view in social science that quantitative and qualitative data are mutually informing (Bryman 2001). Strauss and Corbin agree, arguing that:

> Qualitative and quantitative forms of research both have roles to play in theorising. ... we are advocating ... a true interplay between the two. The qualitative should direct the quantitative and the quantitative feedback into the qualitative in a circular, but at the same time evolving, process with each method contributing to the theory in ways that only each can. (Strauss and Corbin 1998: 34)

However, they stress that, although it is permissible for researchers to use the literature to sensitise themselves to certain issues (1998: 49), it is not permissible to impose a list of preconceived concepts on the data: they must emerge from the data. Preliminary, high-level analysis of the corpus revealed that at least three concepts were ubiquitous: date of each article, the behaviour referred to in the article and the source of the information reported in the article. It became obvious at an early stage that quantitative data relating to these concepts would be important for the study.

Accordingly, the first type of quantitative data used in this study is the date of each individual article which was inserted as part of the file name of each 'primary document'. For example, "1987-05-06 The Times.txt" is the file name assigned to the first UK newspaper article which refers to 'electronic terrorists'. Using the format yyyy-mm-dd was necessary so that all articles were automatically arranged and then loaded into the hermeneutic unit in chronological order. Primary documents could then be sorted into groups by year to allow complex time-based analysis when combined with other codes at a later stage in the analysis.

The second type of quantitative data was generated by assigning certain categories to each article as a whole. It was important to get, so far as possible, an objective view of what types of underlying behaviour were being discussed in the press regardless of the labels assigned in the text. A non-exclusive category of behaviour was assigned to each article, meaning that an article might be referring to more than one category. As a result of the preliminary, high-level analysis, a variety of behaviours was identified which roughly corresponded with the eight main categories derived from the conventional/digital tool/target matrix approach of Devost, Houghton et al. (1997), described in Chapter 2. They use their matrix in the context of terrorist behaviour, but the same matrix can be applied in the context of criminal behaviour. The difference is the underlying intention. This approach produces eight categories as the beginnings of a taxonomy of offending behaviour:

Terrorist activity:

1. Conventional terrorism
2. Conventional tool; digital target
3. Digital tool; conventional target
4. Cyberterrorism

Criminal activity:

5. Conventional crime
6. Conventional tool; digital target
7. Digital tool; conventional target
8. Cybercrime

During the coding process further categories were added as they emerged from the texts and these are described in context in Chapter 5. The categories assigned to each article reflected the basic subject matter of the article as a whole, judged according to the 'real' subject matter of the article and ignoring labels assigned in the text. For example, an article concerning 'cyberterrorist' teenage pranksters who defaced a website is categorised as an article on cybercrime: there is no suggestion of terrorist involvement beyond the label attributed by the author of the article and the acts of the teenagers are technically criminal at English law (Computer Misuse Act 1990).

In addition to the behaviour categories, it emerged that the sources of information used for each article were equally important. For example, was the article predominantly a commentary piece generated from the views of the author himself, or was the material primarily a report of the views of others and, if so, who? Again, 11 codes were pre-defined in this case, so the sources of information gradually emerged from the text. Once again, the categories are non-exclusive, so that one article may be coded as having two or more primary sources. These data are presented in graphical form in Chapter 5 and reveal the major contributors to the public discourse on cyberterrorism.

These were the only types of code which were applied to articles as a whole. All other codes were applied to segments of text, known in Atlas/ti as 'quotations', usually one or more sentences within an article. Initially, an open coding technique was used, essentially to generate qualitative data, but it should be noted here that the third type of quantitative data used in this study comes from the frequencies with which these codes are encountered in the corpus as a whole. These are represented graphically throughout the findings chapters in conjunction with the qualitative findings to illustrate

frequencies of use of various concepts and how they have waxed and waned in importance over time.

(b) Qualitative data

Klein and Myers' fifth principle of dialogical reasoning came into its own when coding the corpus. In the absence of any more obvious strategy, the corpus was coded in chronological order, starting with those texts written at a time when the concept of cyberterrorism was not particularly sophisticated. At the start and, indeed, all the way through the coding process, anything remotely relevant to either hacking, terrorism or both was coded so as not to miss any important nuance in the discourse which might not necessarily be flagged up by the moral panic model. Although it was impossible to forget the model, which had already been carefully researched before coding began, it was possible to put it to one side in the search for anything and everything which might be relevant. Assumptions made at the start of the coding process were repeatedly challenged and modified or abandoned as the process continued and other ideas, not previously guessed at, emerged from the texts and had to be incorporated. As a general example, at the start of the coding process I had a preconception that I would discover the police to be making strong claims about the dangers from cyberterrorism and the powers and tools they would require to address the problem. In fact, as the findings in Chapter 6 show, the police rarely make such claims publicly, preferring instead a restrained and realistic approach. This view emerged from the data and replaced the incorrect preconception at a relatively early stage.

Grounded theory methods are geared towards challenging preconceptions in this way. Data are constantly compared with other data, emerging concepts and categories, and these concepts and categories are similarly compared with the data and with each other. It is a process of constant testing, questioning, affirmation and revision. This amounts to what grounded theorists term 'constant comparison'. This is central to grounded theory methods and it is the mechanism by which concepts are developed, categories and sub-categories formed and theory built. The open coding was deliberately intuitive, the aim being for the researcher to become immersed in the texts to saturation point and to produce the richest possible coding scheme. No regard was paid to the number of codes generated, but it was necessary to know them by heart in order not to miss a coding opportunity when it arose. Constant revision of the coding scheme and revisiting of earlier texts were required to ensure that a concept just 'discovered' had

not, in fact, occurred in an earlier text which had already been coded. This was a very long process and, as noted above, took a little over 18 months to complete.

The next stage in the analysis was to carry out axial coding. Again, it is perhaps misleading to characterise these as distinct stages, rather, they iterated between one and the other and proceeded stepwise. Axial coding is essentially the process of relating categories to their sub-categories (Strauss and Corbin 1998: Chapter 9). Whereas data are fractured during the open coding process, they are reassembled during axial coding so that categories and sub-categories are linked to form explanations about phenomena found in the corpus. Importantly for theory building, the links are made at the conceptual level because the text has, at this stage, been converted into concepts, represented by open codes, which are then reassembled into some sort of order. For example, use of the *future threat scenario* was identified as a dimension associated with three major concepts: *hackers*, the *terrorist link* and *demonisation of technology*. This, then, provided a cross-cutting link between these three concepts and formed a central plank of the eventual theoretical explanation of the social processes at work.

On several occasions, it was found that a particular code was used so frequently that a secondary analysis had to be carried out, resulting in a tree-like structure of coding. Since Atlas/ti only permits two levels of coding – codes and code families – the third level was achieved using a code naming system. For example, the *technology* code was applied to 253 quotations. A more nuanced analysis was required to make sense of the data, so each of these 253 quotations was coded again with several sub-codes using the form *Tech – xyz*, making it obvious that this was a sub-code of *technology*.

The use of memos and diagrams is another technique advocated by Strauss and Corbin (1998: Chapter 14) which is facilitated by Atlas/ti. Perhaps surprisingly, diagrams were not found to be particularly useful in this study, perhaps because the evolving coding scheme turned out to be so highly structured itself. Memos, on the other had, were extremely important. All ideas about the data, codes, how they inter-relate, observations about relationships, indeed anything remotely interesting were recorded immediately as a memo in Atlas/ti. These memos might be freestanding, attached to particular segments of text – perhaps more than one – or attached to codes or code families. They provided a record of the sequence of the researcher's thinking during the analysis and ultimately became the building blocks of the ultimate theoretical explanation of the social processes identified.

What Charmaz terms 'rendering through writing' (Charmaz 2000) was a highly complex process. The decision to start writing up was triggered by the fact that all the texts had been coded, most of them several times over, and it was clear how the coding scheme, representing the concepts which had emerged from the texts, was to be integrated into a theoretical explanation. The writing up process itself was essentially the mechanism by which those concepts were integrated into the theory. In this sense, analysis did not stop when writing up started, indeed a great deal of selective coding (Strauss and Corbin 1998: Chapter 10) continued throughout the writing up process where gaps in the explanation were discovered or where a specific category required integrating and refining. The ultimate goal of these accumulated processes was to reach theoretical saturation, the point in category development at which no new properties, dimensions or relationships emerge during analysis (Strauss and Corbin 1998: 143). This point was not reached until all the issues had been bottomed out and the writing up was complete.

Writing up required the discipline imposed by the meta-structure of the attributional model of moral panic. This was not allowed to interfere with the analysis per se, but was used to organise the approach by isolating a limited number of categories of information for investigation at any one time. This is legitimate, according to Strauss and Corbin (1998: pp 49 et seq) for a number of reasons. The six elements of the attributional model of moral panic can be considered as concepts derived from the literature which provide a source for making comparisons to data at the levels of properties and dimensions. This allows the researcher to identify similarities and differences between the concept known from literature and the emergent concept, thus giving the latter specificity. Another way to consider this approach is that it allowed the researcher to organise the material according to a few themes which were not specific enough to influence the interpretation of the data but were sufficient to give order and direction to a very large body of material. There was no question of forcing the data: this approach was legitimated by the fact that the emergent concepts really did fit the meta structure of the attributional model of moral panic. Finally, where the researcher's intention is to extend an already existing theory, it is legitimate, according to Strauss and Corbin (1998: 50) to engage in research with some concepts and relationships in mind and look for how their properties and dimensions vary under different conditions. This is a good description of what happened in this study. The concepts and relationships described in the existing moral panic literature were indeed compared with

the concepts and conditions which emerged from the specific case of cyberterrorism. Similarities and differences were noted and some modest alterations to the moral panic model suggested. As Strauss and Corbin argue:

> Bringing the literature into the writing not only demonstrates scholarliness but also allows for extending, validating, and refining knowledge in the field. (Strauss and Corbin 1998: 52)

The retrieval mechanisms provided by Atlas/ti came into their own at the writing up stage. Two basic processes were used to consolidate the theoretical explanation and write up the findings. First, the mechanics of coding in Atlas/ti is essentially an indexing process, permitting retrieval of all quotations relating to the particular concept encapsulated in that code. When relevant quotations were read together in one place, rather than being sprinkled across hundreds of newspaper articles, definite patterns emerged which were then integrated into the theoretical model and reported in the findings chapters. Second, a complex retrieval process was used. Because it was decided that the coding structure should be allowed to become as complex as the texts seemed to merit, one quotation was most often coded with multiple codes. Atlas/ti permits retrieval of quotations using a query tool which can combine any number of codes. This resulted in findings in which two or more concepts were related, allowing a rich picture to be built up and integrated into the storyline of the findings.

It will now be apparent that writing up the findings and additional coding cycles were necessarily concurrent exercises because of the iterative nature of the processes of information retrieval and making sense of that information. Reflexivity was paramount and theoretical preconceptions were continuously challenged through constant comparison of concepts and categories, leading to subsequent revisions: essentially the principle of dialogical reasoning in action. The result is, hopefully, a rich picture of the discourse on cyberterrorism using integrated quantitative and qualitative data.

A brief personal insight to enlighten the reader who may find curious my approach to the research design of this study. Whilst acknowledging certain philosophical influences, it was always my intention to come to this research with a clean sheet. Doubtless, there are many other studies which have trodden a similar path to this one. Doubtless, too, I could have fashioned a more elegant approach to my material had I drawn a template for research design from work done by researchers more distinguished and experienced than me. I chose not to do so. We all come to our work with personal motivations apart from the pure desire to know more about our subject. My motivations came as much from the desire to be free from the constraints of the professional legal

environment in which I have been raised, where method and procedure are sometimes even more important than substance; and to exercise my new-found academic freedom in the best way possible: to start from scratch and engage in some blue-sky thinking. I settled on this research design simply because it seemed the best way to do it. When problems came, I rationalised and solved them, always with an eye to analytic integrity and that all-important reflexivity – a skill not entirely alien to the professional lawyer. I wanted simply to set off on the path the data indicated and see where it led. What follows is a summary of how that happened.

SECTION II

THE FINDINGS

The findings of this study are presented in four chapters. Chapter 5, sets out the patterns of reporting on the issue of cyberterrorism in the UK national press; how the press has set the agenda in the debate on cyberterrorism; how it has transmitted associated images and stereotypes; and highlights specific claims made by the press on the subject.

Goode and Ben-Yehuda's attributional model of moral panic (1994) is used to organise the findings in Chapters 6-8. Chapter 6 will present evidence relating to the expression of *concern* about cyberterrorism and the building of a *consensus* about what the problems are. This evidence will be presented from the perspectives of various *claims-makers* in the debate: politicians, agents of law enforcement and national security, the information security industry and other experts. Chapter 7 will go on to consider the evidence on *hostility*: is there *consensus* in identification of the folk devils; how has hostility towards these groups evolved? Chapter 8 will deal with the social reaction to perceptions of cyberterrorism; evidence as to whether or not this reaction is *disproportionate* to the threat; and consideration of the *volatility* or otherwise of the reaction.

A note on the format of these chapters. This study is based on an analysis of a very large quantity of textual data – nearly 700 UK national press articles. The results of this analysis have yielded both quantitative and qualitative data. The former are largely represented in graphical form, this being the most accessible manner of presenting a large quantity and variety of data to the reader. Whilst there will always be attendant explanations, it is intended also that the various charts should speak for themselves.

Discussions of the qualitative findings are punctuated with a large number of quotations from the corpus. This may look unconventional to the reader. However, the findings have been put together in such a way that the quotations flow logically with the commentary. They are intended to be read as part of the narrative, illustrating a point and adding a fresh dimension to the argument. This prevents the need for undue repetition so that, where a quotation in its context makes a point, there is no need to rehearse that point again in the attached commentary. Importantly, this use of quotations substantially avoids the risk of over-interpreting the material and adding

personal biases (Hosein and Whitley 2002) by making plain the meaning of the original text and forcing the researcher to greater reflexivity. Although a large proportion of the chapters which follow are made up of quotations from the corpus, it is the choice of quotations, their logical ordering and the manner in which they are woven into a coherent narrative which represents the task undertaken by the researcher. This study, based as it is on textual material, requires such a format in order to provide sufficient evidence for the arguments being made. Exemplar quotations are limited to two or three at most in each case, although many more examples can usually be found in the corpus.

CHAPTER 5

FINDINGS:
BRINGING THE DEBATE TO THE PUBLIC: THE UK NATIONAL PRESS

Cohen has identified three main rôles for the media: agenda setting, image transmission and claims-making (Cohen 2002: xxiii). This chapter will set out the position of the UK national press in relation to each of these three rôles in the context of the narrative on cyberterrorism.

1. SETTING THE AGENDA: THE ASSOCIATION OF HACKING AND TERRORISM

An analysis of the quantity of UK national press articles over time shows that there has been a striking rise in the reporting of hacking and terrorism together, from a total of three in 1997 to 81 in 2005 (Figures 1 and 2). A total of 681 UK national press articles make up the corpus of data for this study. The absolute figures are relatively low in comparison with reporting of computer hacking without mention of terrorism (Figure 3) which also display a clear upwards trend over time, with over 800 articles mentioning hacking in 2005, although these have not been filtered for duplication and relevance. The significant peak in 2000 is explained by a series of high-profile hacking incidents which made headlines across the world: the Mafiaboy denial of service attack on eBay, Yahoo et al; the spread of the 'I Love You' virus; a rash of website defacements by Pakistani and Middle Eastern 'hacktivists' protesting against India and Israel respectively; Microsoft's admission that hackers had accessed the source code for the next release of Windows and Office; and the FBI arrest of two notorious Russian hackers. Nevertheless, when the number of articles on hacking and terrorism together are considered as a proportion of the number of articles on hacking alone, over time there is a clear upwards trend, which demonstrates that, of all articles which consider hacking, the proportion which associate hacking with terrorism is getting larger year on year (Figure 4).

As Figure 2 demonstrates, press interest peaks at certain points, and this tends to indicate peaks of interest in a given episode. For example, the peak in 1996 Q4 is explained by reporting of alleged IRA access to personal information on potential

Figure 1 **Frequency of UK national newspaper articles citing hacking and terrorism, by year**

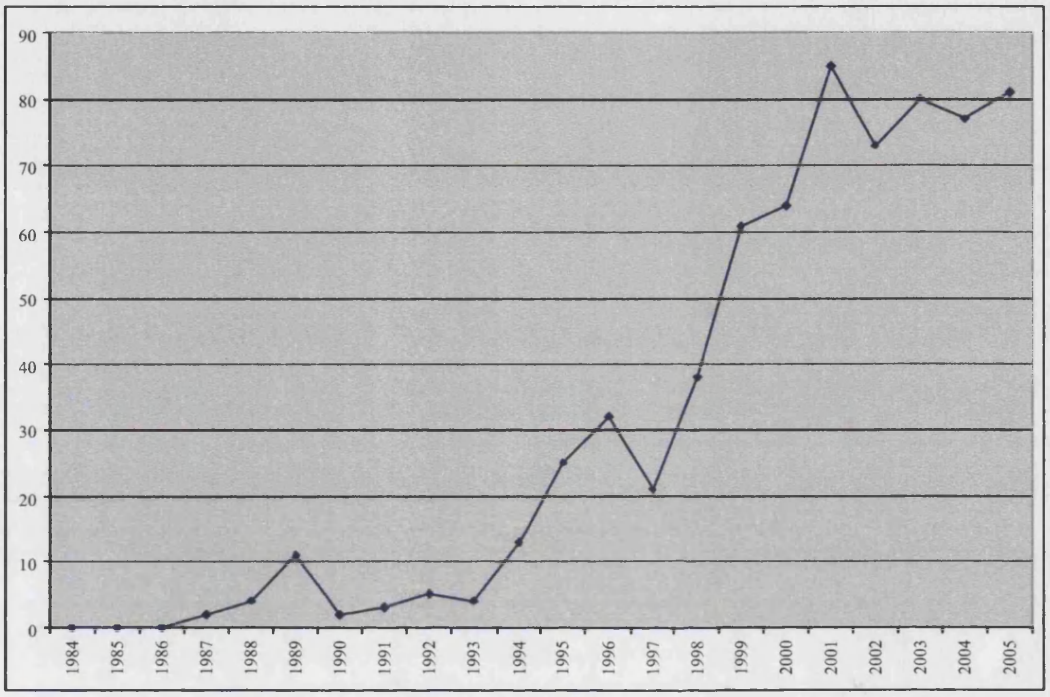


Figure 2 **Frequency of UK national newspaper articles citing hacking and terrorism by quarter, with 8 quarter moving average trendline**

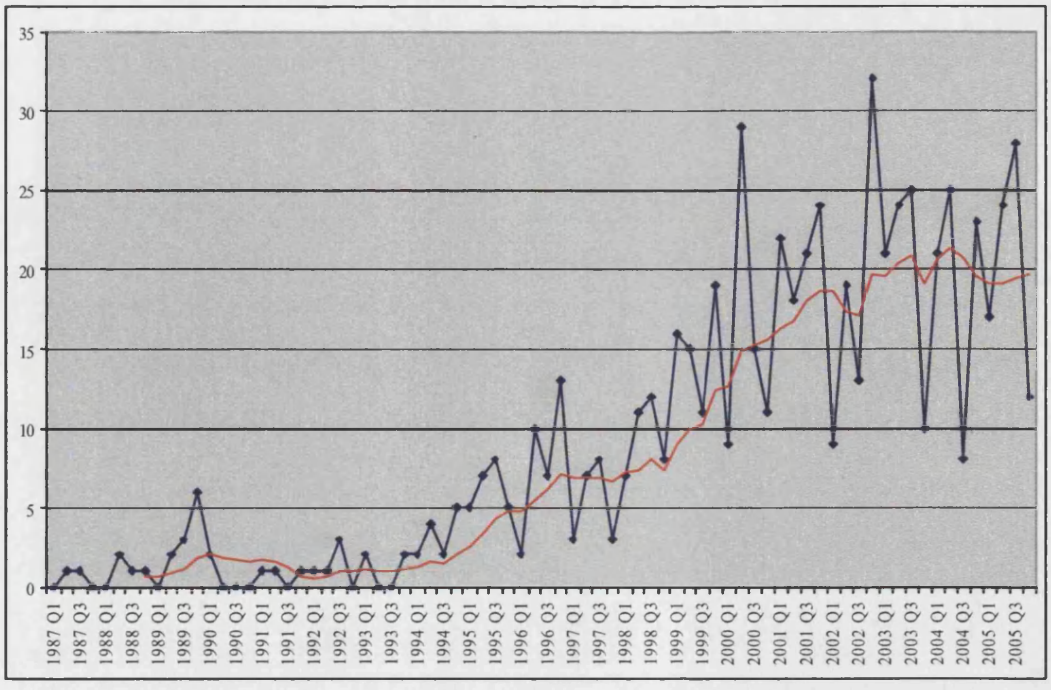


Figure 3 **Frequency of UK national newspaper articles citing hacking and terrorism and articles citing hacking only, by year**

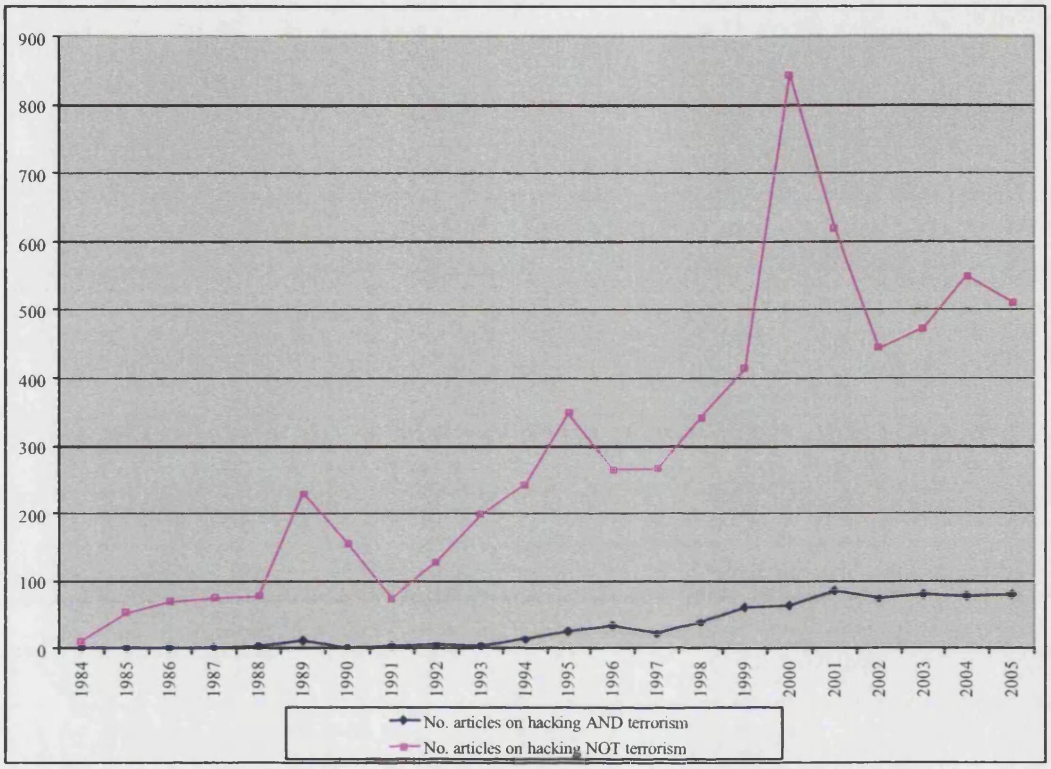
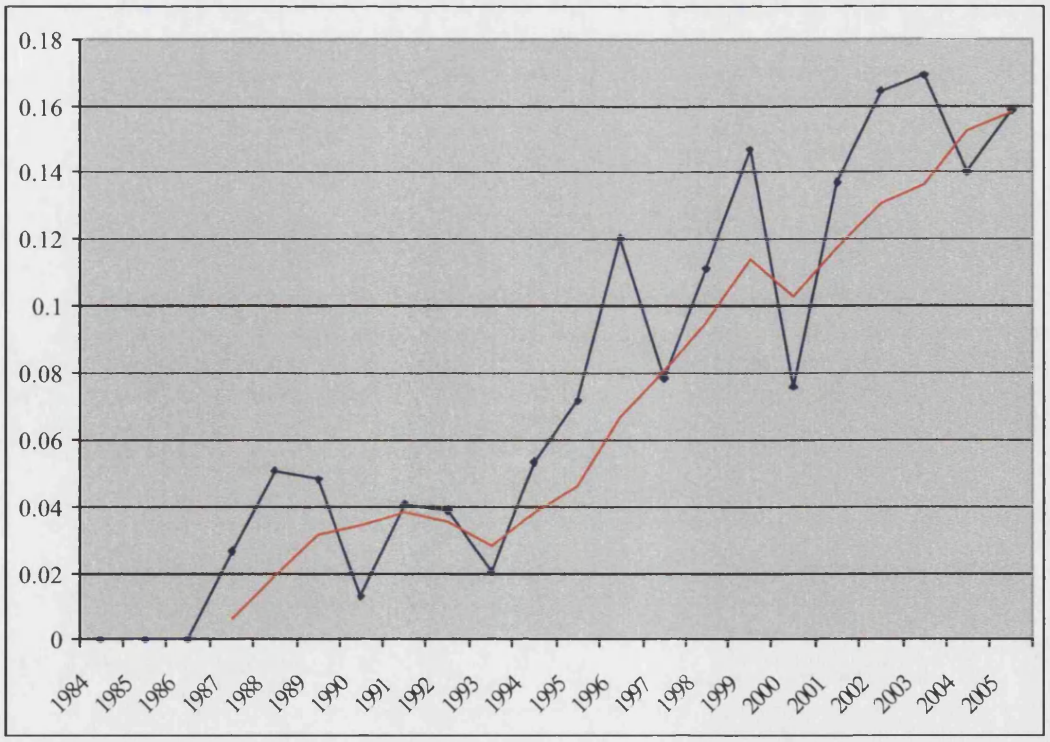


Figure 4 **Ratio of number of articles citing hacking and terrorism to articles on hacking by year, with a 4 period moving average**



targets, gained by 'hacking' corporate records, although in most cases company insiders were involved and the terrorists were not hackers at all. Another significant peak in 2000 Q2 is explained by the 'I Love You' virus, which caused widespread havoc across the Internet. Its originator was branded a cyberterrorist. The peak in 2002 Q4 is largely explained by the attempted extradition to the US of a UK hacker who hacked US military computer systems over a period of months. There were widespread rumours that he had terrorist links because he was active around 11 September 2001. At subsequent court hearings in the extradition case, press interest peaked again, notably in 2005 Q2 and Q3.

Perhaps these increased reporting patterns are correlated with increases in underlying behaviour, with terrorists more frequently engaging in hacking and hackers turning to terrorism. However, close examination of the corpus reveals no reports of genuine cyberterror attacks, so another explanation must be sought for the association of hacking and terrorism in the national press. To understand the increased frequency of reports, it is necessary to consider their actual subject matter: of those reports associating hacking and terrorism, how many are discussing cyberterrorism (as defined in Chapter 2), and how many are discussing other issues? During the coding process, the articles were sorted into non-exclusive categories of behaviour, meaning that an article might be referring to more than one category. As described in Chapter 4, the (one or more) categories assigned reflected the basic subject matter of the article as a whole, judged according to the 'real' subject-matter of the article and ignoring labels assigned in the text. At the start of the coding process, there were the eight main categories:

Terrorist activity:

1. Conventional terrorism
2. Conventional tool; digital target
3. Digital tool; conventional target
4. Cyberterrorism

Criminal activity:

5. Conventional crime
6. Conventional tool; digital target
7. Digital tool; conventional target
8. Cybercrime

During the coding process further categories were added as they emerged from the texts. These categories relate to activities outside the criminal and terrorist mainstream, but were nevertheless popular in the corpus.

9. Accidental damage

These were articles where the main focus was on damage to information systems which had, in reality, been inflicted accidentally.

10. Communication

The activity described was generally of a non-destructive nature, such as using the Internet for communication, propaganda, recruitment. Some destructive activities were included, such as the so-called 'hacker wars' which amounted to little more than tit-for-tat website defacements by, for example, Israeli and Palestinian hackers. Reports of such activity were included in this category where the main reason for the website defacement was promotion of propaganda, although they may additionally have been coded as "8. cybercrime".

11. Ethical hacking

This is the name often used where a person gains access to parts of an information system which he should not have access to, but then informs the organisation of its vulnerabilities. The tag is also applied to similar techniques used within the information security industry with the full permission of the target organisation.

12. Information warfare

This category started to come to prominence in the late 1990s. It includes reports concerning information warfare between nation states, such as security services of one state disrupting the dealings of another which is suspected of aiding terrorists. It also includes industrial and state espionage. Post-9/11 reports on hackers working for Governments against al-Qaeda were also added to this category.

13. Hoax

This category refers to a genuine hoax situation. A frequent example is emails claiming to be virus warnings, which heighten fear and concern without there being any actual cause. Not to be confused with hoax emails pretending to be something legitimate but which actually contain a virus: these are category 8 (cybercrime).

This analysis of the articles in the corpus provides the distribution of their subject matter as objectively determined, rather than as determined by reference to the language used in the article. The results are presented in Figures 5 and 6. Figure 5 demonstrates

that a significant majority of articles which associate hacking and terrorism are really reporting criminal issues. The number of articles which actually report terrorism as part of the main subject matter is roughly a third of the number of those reporting crime. The remainder of articles principally reports issues other than crime and terrorism. It follows that the terrorism issue is often introduced into articles which deal predominantly with crime, without it being pertinent to the fundamental subject matter of the article.

Figure 5 **Frequency distributions for categories of 'terrorism', 'crime' and 'miscellaneous' which are further broken down in Figure 6**

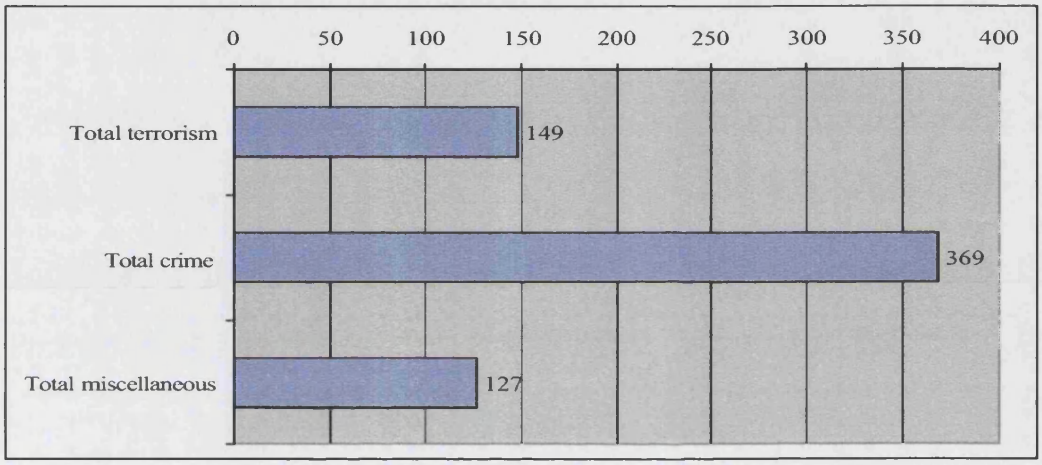
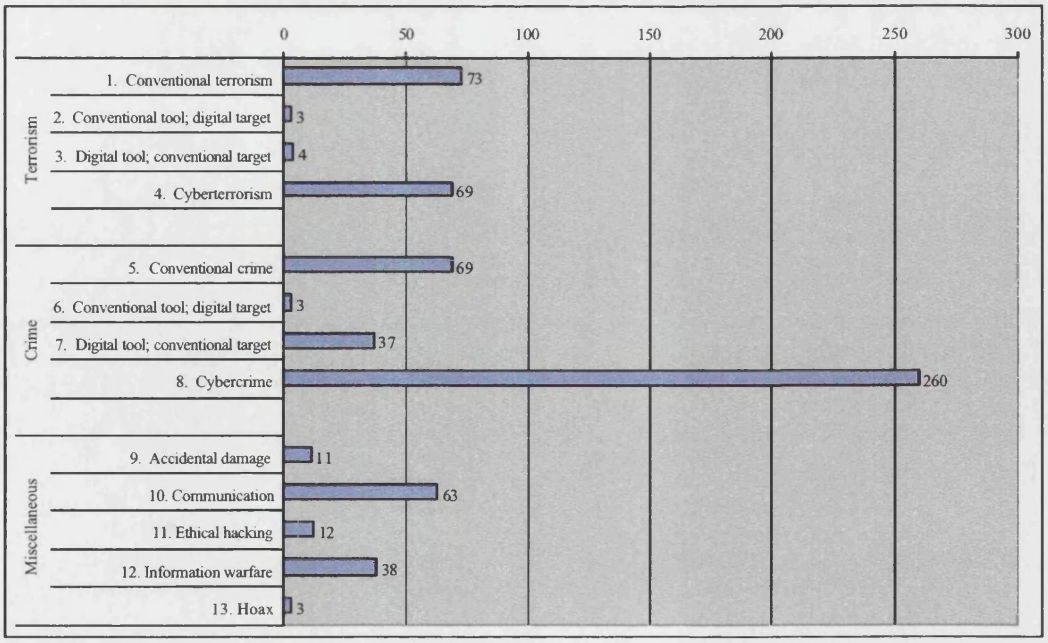


Figure 6 **Frequency distributions for non-exclusive behaviour categories described in articles citing hacking and terrorism**



The striking feature of the frequency distribution of the behaviour categories presented in Figure 6 is that 250 articles from the corpus of 681, representing over one third, are reporting on cybercrime specifically, even though all of these articles bring up the terrorism issue. This is nearly four times more than the next most popular categories of conventional terrorism, cyberterrorism, conventional crime and communication. Two further categories are worthy of specific mention, crime using digital tools to attack conventional targets, and information warfare. The nature of the reporting of these behaviour categories will be explored in the remainder of Section 1 to establish the context in which the terrorism issue is introduced. The discussion is emphatically in relation to the stance taken by the press as a claims-maker in its own right, rather than press reports of claims made by others, which are discussed in Chapter 6.

1.1 Cybercrime

Ordinary criminal activity is overwhelmingly the most common behaviour described in articles citing both hacking and terrorism. In most cases, the issue of terrorism is introduced to 'spice up' an otherwise mundane report of everyday criminal activity. Under the headline "*Computer terrorism 'coming to Britain'*", *The Independent* claimed:

> Bizarre new corporate computer crimes, including terrorism by electronic mail and "fax graffiti" attacks, now rife in the US, are coming to Britain, specialists warned yesterday. ...
>
> In the US, at least 80 prosecutions are being brought for acts of electronic terrorism. These include cases in which offenders ring in to a company voice-mail system and leave threatening messages. *28 November 1991*

Threatening voicemail messages, whilst undoubtedly unpleasant, do not, on any balanced analysis, amount to terrorism. A *Sunday Times* headline warns '*Secret DTI inquiry into cyber terror*":

> The government has been holding a secret investigation into attacks by 'cyber terrorists' on the City of London for more than two years. ...

Later in this article a DTI statement makes it clear that the 'cyber terrorism' actually refers to suspected extortion, a simple (albeit serious) criminal offence:

> ... We are very interested in the allegations of extortion directed at City of London institutions which were brought to our attention in 1994. ... So far, we have not been presented with any hard evidence from victims. *The Sunday Times, June 9, 1996*

Once again, exaggeration is being used in order to make the piece more exciting. *The Mail on Sunday* resorts to 'what if' tactics to introduce terrorism, starting with a story about ordinary hack attacks on government systems and then finding an expert to extemporise on the possible consequences if terrorists ever started hacking:

> The staggering discovery that growing computer terrorism could destabilise Western governments has led to an international inquiry. European political leaders are so concerned at the ease with which government computer systems can be infiltrated by hackers that they are now demanding urgent action. ...
>
> Amazingly, all the organisations and governments infiltrated in recent years have remained ignorant of their vulnerability to electronic terrorism - even when the hackers actually 'controlled' their computer systems. ...
>
> One computer expert said: 'Up to now most of the hacking has been done for fun but if the know-how of these people ever fell into the wrong hands - those of terrorists or political extremists - the consequences could be catastrophic. ...
>
> The grim potential for terrorist gangs or sinister political groupings to hold the world to ransom through computer sabotage has not been lost on political leaders worldwide. *14 February 1993*

After 9/11 the issue of terrorism gained greater momentum and it coloured reporting of a variety of ordinary criminal incidents. Tabloids were particularly keen on this kind of presentation, although the broadsheets were by no means averse. *The People* claimed "*Terrorists in e-mail plot*":

> Security chiefs fear that followers of Osama Bin Laden have turned to cyber terrorism in a plot to paralyse Western governments.
>
> Mystery hackers have spread a highly destructive virus through the European Parliament's e-mail network. Now there are fears it could be passed on to government systems all over the world.
>
> One Euro source said: "This could be the work of al-Qaida terrorists." *June 16, 2002*

It seems that a 'source' can be found to support most claims yet, in this case, there was no reason to assume that this virus originated with a terrorist organisation.

Sometimes the issue of terrorism is introduced because there is a genuine, if misguided, belief that the attack in question was carried out by terrorists. A letter from Emma Nicholson, MP claims:

> I have been told by security sources that extremists in Holland and Germany have used computer-derived information to bomb oil refineries and destabilised government actions.
>
> With such a background no 'special case' consideration can be retained for the hacker. Those 'innocents' who claim immunity must realise that they stand in the company of the international terrorist and industrial blackmailer. *The Independent, 30 December 1989*

Nicholson was sponsor of a Private Member's hacking Bill which later became the Computer Misuse Act 1990. Sometimes such claims are made cynically, however. In 2001, even before the World Trade Center attacks, Michael Vatis, then Director of the US National Infrastructure Protection Center, claimed:

> Hackers come in a variety of flavours, from the unwitting teenager messing about on a home PC, who, "doesn't usually mean any harm but ends up causing millions of dollars

> worth of damage," to the Bin Ladens of this world. *The Daily Telegraph, 1 March 2001*

Although terrorist use of the Internet for communication, propaganda, fund raising and other ancillary purposes are reasonably widely accepted, there has been no credible claim that Bin Laden or his associates have used the Internet for cyber-attack. As Director of the NIPC, Vatis would have known this well. His cybercrime unit was at this time newly established under Bill Clinton and this may explain why he was 'talking up' his remit.

There are endless examples of how terrorism is worked into mundane reports of computer-related crime, and a flavour is given here. For present purposes, note that, of 681 news articles citing both hacking and terrorism, the vast majority are of this nature and, in reality, report nothing more than mundane, computer-related crime.

1.2 Conventional terrorism

Amongst the articles predominantly discussing terrorism, there is a roughly equal split between conventional terrorism and cyberterrorism (Figure 6). Hacking is often linked with conventional terrorism because the resulting issue of cyberterrorism is thought to capture the imagination of the reader. For example, towards the end of 2004, *The Independent* prints the headline "*CBI Annual Conference: head of MI5 warns business to guard against terrorism*", and largely discusses defences against the consequences of conventional terrorism, but goes on to report:

> A security specialist with Sun Microsystems, a software company which designs measures to combat "cyber-terrorism" disclosed that in almost a third of companies former employees still had access to internal computer systems. *17 November 2004*

This had nothing to do with the terrorist angle of the story, but seems to have been thrown in for good measure as a hot topic. Sun Microsystems deal with information security generally, not terrorism in particular. The word 'cyber-terrorism' is used in place of the rather more mundane 'cybercrime' or 'hacking'.

1.3 Cyberterrorism

When cyberterrorism in its technical sense is reported, the predominant theme for discussion is the *potential* for cyberterrorism. In this study, this is termed the 'future threat scenario': an event or state of affairs is specified and this is used as evidence that electronic catastrophe is inevitable and, often, imminent. The specified event or state of affairs used as evidence for the future threat scenario changes over time. A fresh round of concern might be triggered by an event such as the emergence of a new technology, the publication of a report or a declaration of war. The importance of scenario-building

is elaborated further in the next chapter, but the following example is representative of the general approach taken by the press:

> Extremists are recruiting Islamist computer hackers – creating a breed of high-tech terrorist who threatens to cripple Britain's economic infrastructure.
>
> Banks, businesses, Government offices and transport systems are in the frontline of a new wave of cyber terrorism that could bring the country to a standstill and drain billions from the economy. *Sunday Express, 30 October 2005*

A somewhat lesser, although significant, proportion of articles which discuss cyberterrorism are dealing with policy issues – the formalised social reaction to perceived risks.

> Among the Marsh commission's recommendations are a doubling of spending on combating computer terrorism (from the current £160m), the formation of an office to assess the potential threat to computer networks in public and private sectors, and enhanced co-operation between the private computer sector and government departments. *The Independent, 22 October 1997*

On proposals for the Terrorism Bill, later the Terrorism Act 2000:

> The Government also plans to adopt the FBI's definition of terrorism as being violent acts carried out by groups such as militant computer hackers and some anti-abortionists. *The Times, 18 December 1998*

And when the Act came into force:

> It also targets "cyber terrorists" who cause serious disruption by attacking computer installations or hack into electronic data to undermine governments or threaten lives. *The Daily Telegraph, 19 February 2001*

1.4 Conventional crime

Crime is classified in this study as conventional, rather than cybercrime, where there is only a weak association with computers, and the most frequent crime in this category is blackmail or extortion. Once again, terrorism and a computer angle are added to sensationalise reports. This passage describes some sort of intimidation, but there is no reason to assume that the activity is carried out by terrorists or for terrorist motives:

> In the US, at least 80 prosecutions are being brought for acts of electronic terrorism. These include cases in which offenders ring in to a company voice-mail system and leave threatening messages. *The Independent, 28 November 1991*

The crime described in the next passage is blackmail, but because of the threat to destroy computer systems, *The Observer* elevates the status of the blackmailers to "cyber-terrorists":

> Cyber-terrorists are reported to have blackmailed British and US financial institutions to the tune of pounds 400 million by threatening to wipe out their computer systems. *The Observer, 2 June 1996*

In a different story from *The Daily Mail* similar tactics are used in the headline:

CYBER TERRORIST STRIKES; Defence chiefs 'blackmailed' as hacker targets satellites and security posts. *Daily Mail, 1 March 1999*

1.5 Communication

These articles often report terrorist use of ICTs, which is not considered cyberterrorism within the definition used in this study. Bin Laden is frequently reported as a heavy user of technology:

> Technology allows information to be encrypted into webcasts...
>
> Osama bin Laden is an expert at transmitting his views by video - to the point where the Pentagon wondered whether they might contain secret messages. *The Times, 13 December 2001*

There were also allegations of cyberterrorism in relation to the Bali bombing, although these were mainly to do with use of the Internet at the planning stage:

> FBI investigators fear the outrage was al-Qaeda's first cyberwar attack.
>
> Defence specialists believe Osama bin Laden fanatics planned and executed the bombing using computers.
>
> The masterminds could even have detonated their devices from thousands of miles away, possibly Pakistan or Kashmir.
>
> The CIA have established that bin Laden ran many of his earlier operations over the internet. *Daily Star, 15 October 2002*

Another significant proportion of the communication category relates to propaganda-motivated activities by activists or other non-terrorist groups who are often characterised as terrorists.

> The information terrorists at Undercurrents.org have been around for a while putting out their particular brand of social justice activism, which centres around making videos documenting grass-roots struggles, protests and actions from around the globe. *The Guardian, 24 April 2003*

A further example is provided by DK Matai of Mi2g who is a frequent 'expert' source of the more outrageous claims about cyberterrorism. Here he refers to the web defacements which occurred during the Balkan War:

> DK Matai, managing director of Mi2g, said: "The internet attacks from pro-Serbian elements highlights, for the first time, political activism as a force for cyber terrorism." *The Sunday Times, 15 August 1999*

1.6 Crime: digital tool, conventional target

There is an important distinction to be made between cybercrime and conventional crime in which a computer happens to be used. DS Don Randall, of the City of London Police fraud squad, summarises these distinctions succinctly:

> ... it was important to distinguish between a crime in which computers were used as a tool, and computer fraud, which involved manipulating or corrupting a mainframe, which was still relatively uncommon.

> 'There is very little computer fraud as such, but almost any fraud has now got an electronic aspect,' he said. *The Independent, 10 October 1989*

There is a further fine distinction between what counts as conventional crime, as discussed above, and what counts as 'digital tool, conventional target' crime. The general criterion used when coding was that, for this category, a computer was actually used in the commission of a conventional offence, such as using a denial of service attack to extort money from a commercial organisation, or gaining access to confidential information through hacking. Certainly, DoS attacks and hacking are cybercrimes in their own right but, in these cases, they are actually means to a more conventional end.

The issue of terrorism tends to be introduced into articles falling into this category by means of the 'what if' mechanism. A criminal innovation is detailed, examples are given, then there is speculation on what might happen if terrorists started doing the same:

> Hordes of web bots do crooks' bidding: Malicious Programs threaten to engulf UK corporations as hi-tech crime taskforce tracks cases of online blackmail around the world.
>
> ... Financial crime is not the only concern. Terrorists could use such techniques to try to paralyse an emergency telephone network or an air traffic control system, with devastating consequences, particularly if combined with a physical attack. *The Guardian, 13 November 2004*

This extract is interesting because it provides a good example of how the police sometimes use the voice of reason, allaying fears and dampening panic. Other examples play on existing fears, such as the following example detailing notorious security flaws in Microsoft products, and add the spectre of terrorism to emphasise the point:

> The Government was accused last night of leaving Britain's nuclear arsenal wide open to terrorist computer hackers.
>
> MPs and computer experts demanded answers from Defence Secretary Geoff Hoon after claims that the computers on our nuclear submarines are to be run on the Windows 2000 system.
>
> They allege that the software, which runs many home computers, is vulnerable to attack by hackers. *Sunday Express, 24 October 2004*

1.7 Information warfare

The information warfare articles are a curious mixture and reflect a growing concern in the press which manifests from the late 1990s onwards. This category includes industrial and state espionage. Given that this study is not focussed on information warfare, as such, it was not thought necessary to separate the issues of espionage and

information warfare which, in any event, overlap to a certain extent. Moreover, the boundaries between the state and global business interests are increasingly blurred, so that damage to one may affect the other. The coding term "information warfare" is, for this reason, taken to cover both state and business interests.

Here, again, terrorism is most often associated with information warfare through the 'what if' mechanism. As exemplified here, the argument is often based on the advantages terrorists might find in new techniques of asymmetric warfare:

> I-War is a great equaliser. The more technologically evolved you are, the more vulnerable you are. And no matter how backward your country may be, how unsophisticated your means of conveying utilities or waging conventional war, you can be David to the American, or the Western European, Goliath. This is a form of war that a Third World rogue state, or a small terrorist organisation, could wage against the mighty superpower and win - or, at any rate, not lose. *The Independent, 22 February 1998*

Summary

Of the 681 UK national press articles, all of which associate hacking with terrorism in some way, at least 57% are fundamentally dealing with the subject of crime, computer-related or otherwise. Of the remainder, 12% discuss some form of conventional terrorism, which may include a computer-related element, 10% discuss communication, and 6% discuss information warfare.

11% of the articles studied have as their principal focus the subject of cyberterrorism, as defined in Chapter 2. The important message is that hacking and terrorism are often associated in a corpus of press articles which are predominantly reporting mundane, computer-related crime. This is evidence of concern, yes, but it is also evidence of attempts by various actors, including the press, to entrench the association of hacking and terrorism in the generalised belief system which is growing up around hackers, terrorists and the Internet. This despite the fact that the reports reveal neither evidence of hackers being associated with terrorist groups, nor evidence of terrorists using computers and the Internet for anything more than communication or criminal activities, such as fraud and counterfeiting. The press are clearly setting an agenda by deliberately constructing a link between hacking, terrorism and technology and often explicitly calling it 'cyberterrorism'. This style of inflammatory reporting raises awareness and puts cyberterrorism on the map of social problems, about which 'something must be done'.

2. IMAGE TRANSMISSION: REPORTING THE CLAIMS ABOUT HACKING AND TERRORISM

As well as agenda-setting, there are two further rôles which may potentially be taken on by the media: image transmission and claims-making (Cohen 2002: xxiii). This section will consider the sources of the images transmitted by the press, and Section 3 will discuss claims made by the press as claims-maker in its own right. The substance of the claims made by other claims-makers is left for Chapter 6.

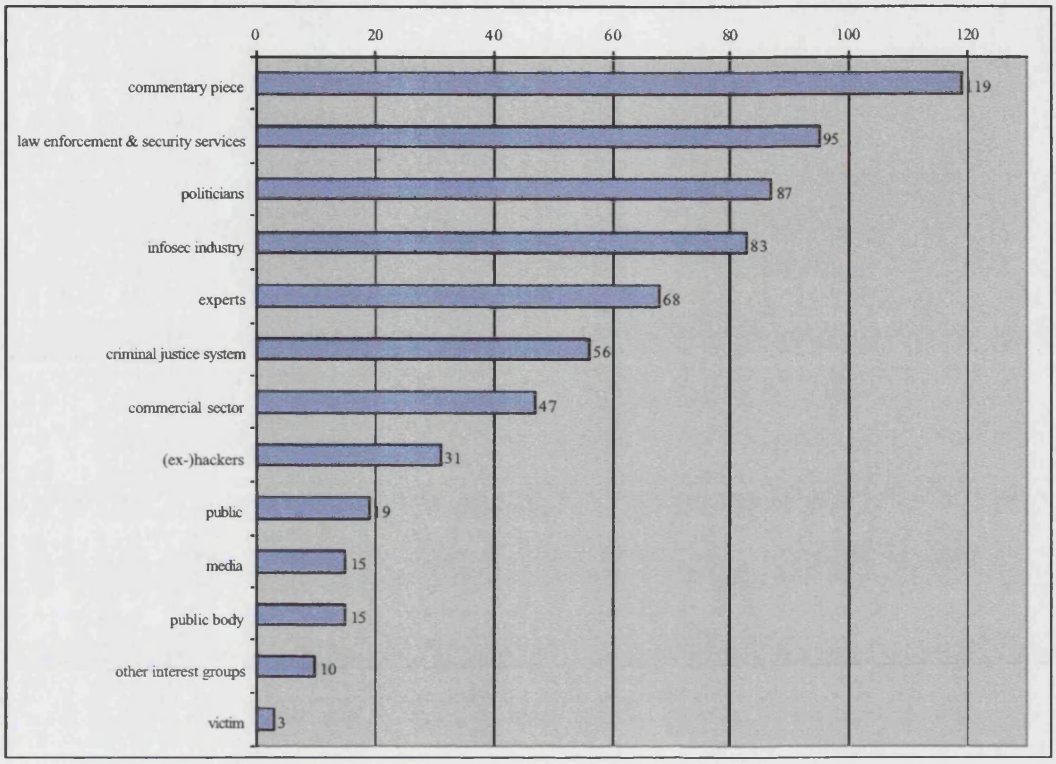
First, which claims-makers are represented in the UK national press? Just as the articles were sorted into non-exclusive categories of behaviour during the coding process, the source or sources of information for the article were also identified. Once again, the sources are non-exclusive categories, and more than one source was assigned to an article if appropriate. A 'source' in this sense refers to a 'claims-maker' in moral panic terminology. The data collected from the corpus and presented here establish which individuals and organisations are acting as claims-makers in the cyberterrorism narrative.

Figure 7 shows the number of articles associated with each source category. This is a measure of the general influence of each source in the UK national press. Figure 7 demonstrates that the press functioning as claims-maker provides the impetus for more articles than any other source. These are instances where the writer of the article is himself making claims about the problematic situation, either amplifying or attenuating the rhetoric of cyberterrorism. The actual claims made by the press will be discussed further in Section 3.

Not far behind are the triumvirate of law enforcement, politicians and information security industry. Claims-makers in the law enforcement category include intelligence services and military, as well as police. They are grouped together for the purposes of macro analysis because their claims are remarkably similar and have enormous influence with the press. Differences in motivation emerge at the micro level, and these are discussed separately and in historical context (Chapter 6). The most influential political claims-makers reported in the UK press are UK and US politicians, both highly active in the area of cyberterrorism. The information security industry is a top claims-maker but it is, perhaps, surprising that the industry comes behind law enforcement and politicians.

So-called experts are also highly influential and may come from industry, academia, voluntary organisations, the public sector and elsewhere. They are called upon by the

Figure 7 **Frequency distributions for non-exclusive source categories for articles associating hacking and terrorism**



press, politicians and others when it is necessary to provide evidence for a particular viewpoint. They are important because their expertise is socially accredited and their pronouncements give credence to the claims being made about a problematic situation. Not only do they warn about the nature of the problem, but they also propose solutions. 'Experts' are often quoted in the press without any indication of who they are or what their affiliations are. In a sense, who these experts are is of limited importance because it is their status, rather than their job description, which gives force to the rhetoric they are asked to support. Their expertise is often not so much inherent as attributed by the press.

Further down the list of influential claims-makers comes the criminal justice system, not including the police. Sources from within the criminal justice system tend not to be claims-makers, as such, but reports of court proceedings and the like, thus a 'source' of a story in the more traditional sense. Less frequently reported claims are made by sources in the commercial sector, representing commercial interests outside the information security industry. An example would be a spokesman from a business association such as the CBI. Victims of cyber attack come at the bottom of the list. This is likely to be because high-profile victims are unwilling to discuss their

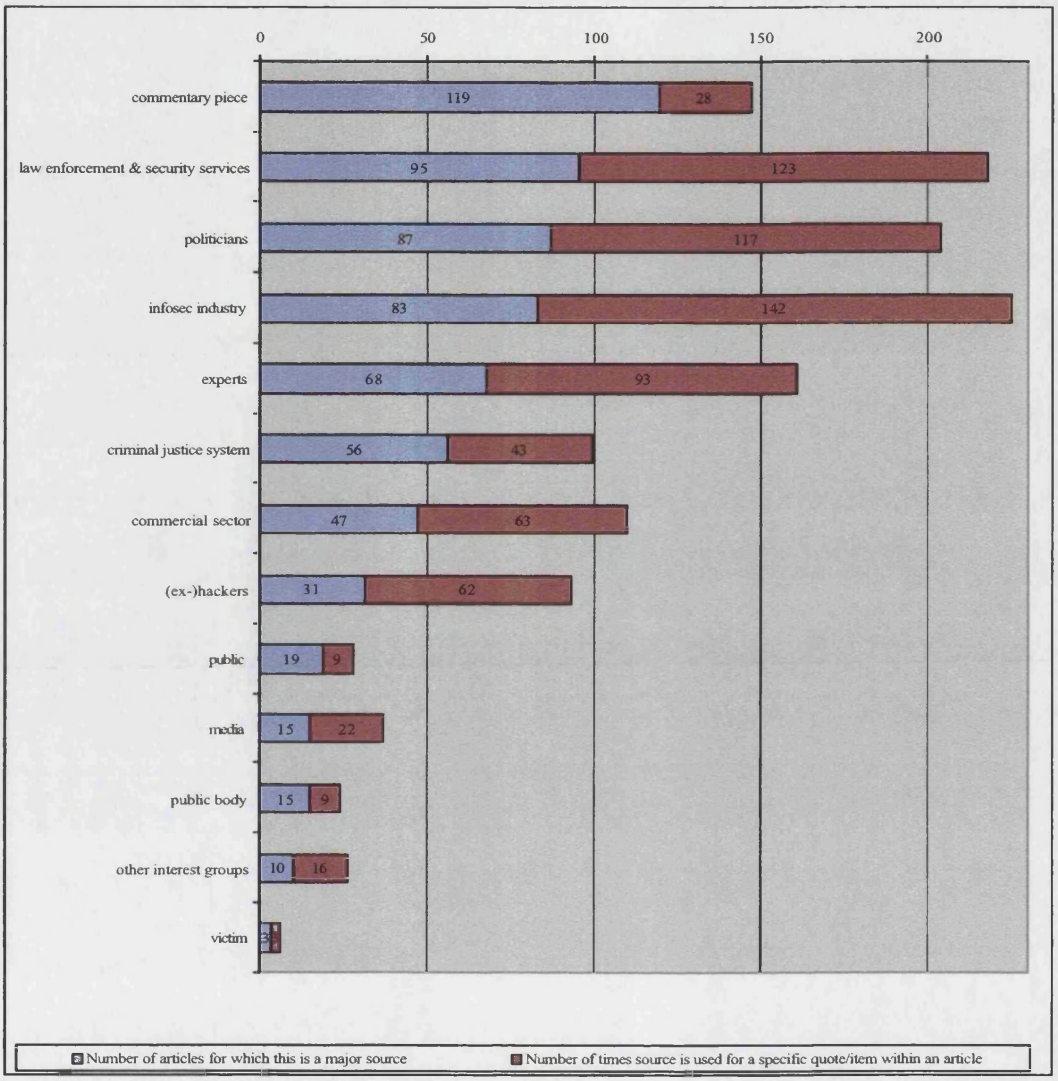
experiences because of the stigma attached to security breaches. Low-profile victims, on the other hand, are unlikely to be deemed newsworthy.

Hackers, both former and current, feature in the list of claims-makers but are not regularly reported. This deviant group has not found a powerful voice in the press. Terrorists, perhaps unsurprisingly, do not act as claims-makers at all. This is important because it demonstrates how claims about cyberterrorism may remain uncontested. If the 'deviant' group cannot or will not speak up for itself, only elements from within the other claims-making groups can speak on their behalf.

The codes relating to the source of a claim were also used for individual text segments as well as entire articles. An example would be a quotation in the text of an article which was directly attributable to a particular source, such as a government minister or a police officer. This is a measure of frequency of citation of, or reference to, the particular source in the UK national press. It is possible to split the source codes referring to articles as a whole from source codes referring to text segments. If Figure 7 gives the data relating to the former, Figure 8 shows these same data, together with the data for the text segments.

The aggregate data in Figure 8 are important because they show how influential a particular source is overall, both in terms of general influence and frequency of citation. According to these data, the four main influences in the UK national press change. There are two significant results. First, when direct quotations and references are taken into account, the influence of the information security industry in press reporting of hacking and terrorism is greatly increased. This suggests that the press uses the industry as its primary source of 'experts' (represented by the data in purple) as well as reporting more passively the claims made by the industry (represented by the data in blue). Second, the overall importance of the press itself as claims-maker is exposed as being somewhat less than might previously have been supposed. This suggests that the press is not necessarily driving the majority of what is written on cyberterrorism in terms of claims-making and that reports are more often reactions to claims that have been made in public and which editors deem newsworthy. Certainly, there is a filtering mechanism at work here and the press still wield considerable power over this issue, but other actors, such as industry, law enforcement and politicians, are self-evidently engaging in the dialogue.

Figure 8 **Aggregate frequency distributions for sources influencing an article as a whole and for sources quoted or referenced specifically in the text**



Summary

Although the press has a voice of its own, it is predominantly engaged in transmitting the rhetoric of other claims-makers as part of its image transmission rôle. This gives high profile and circulation to the views of key claims-makers in the cyberterrorism narrative. However, the press are not neutral in this process: on the contrary, the rhetoric of others is often either amplified or attenuated, leading to a body of reports which are substantively heterogeneous.

3. THE PRESS AS CLAIMS-MAKER

This section examines the claims made by the press itself and the themes which arise in its presentation of cyberterrorism. Before considering these questions in detail, as with any other claims-maker it is worth investigating the particular motivations of the press.

Peter Sommer, writing as Hugo Cornwall and an expert frequently called upon by the press, puts it vividly:

> When journalists ring you up with their rumour of a hack, their report of evidence of eavesdropping by VDU radiation, their 'steer' from the authorities of a computer fraud about to be frustrated, their anxiety that every other journalist in town is writing about computer viruses, or about subversive or pornographic bulletin boards, what they really want is a validating quote for a slightly rickety story. They can only use your views if they are sensational. Tell the newshounds what you honestly think, and either the story dies or they rush back to the contacts list until they find a more quotable expert...
>
> I suspect that the real losers from all these misleading press stories are computer users who protect their systems from dangers they don't really face whilst ignoring more mundane, and real, perils. *The Guardian, 5 May 1988*

Sensationalism is a significant driver behind many press reports. Basic computer-related crime is often dressed up as 'cyberterrorism' for added effect. Yet the tone of press reporting is not homogeneous, and those instances where the press acts to attenuate the rhetoric of panic will be considered first. This may be by way of direct comment by the author, and the point is often an important one about policy and what kind of society we want to live in:

> ... the Internet has been represented as a potential site for major calamities. There has been much press comment about so-called 'cyber-terrorism' and the threat to society's moral well-being from pornography and paedophile rings...
>
> Research shows that although anxieties about risk are often disproportionate to the real dangers facing us, they can have a major impact on the way we conduct our life. *The Guardian, 26 July 1997*
>
> The ... proposal [made by academics in a recent issue of Foreign Affairs] also suggests a National Information Assurance Institute... It would guard against cyber-terrorists spreading computer viruses and trade information before tipping off government. But such an institute would have a huge pool of confidential information - medical records, credit ratings, telephone records. Who guards the guardians?
>
> Europeans should listen carefully to this US debate and question its assumptions. It is all right for Hollywood to imagine an evil mastermind striking at society. But it is another matter to base a hi-tech backed strategy on such an ill-defined threat. Given shrewd political guidance, existing agencies, acting within present laws, can provide a shield against catastrophe. *The Times, 16 January 1999*

Often, the attack is a more personal one, focussed on politicians with ulterior motives:

> If you believe Robin Cook, the main threat we face from computers is "hacking". Cyber-terrorism, he warned his parliamentary colleagues, can "cripple Britain faster than a military strike".
>
> It seems that Cook, like Ronald Reagan before him, has been reading too much Tom Clancy. Or, more likely, he knows that if you frighten the pants off us we may not ask awkward questions about the bill for £2.5bn that MI5, MI6, and GCHQ is presenting to British taxpayers for the privilege of having their email spied on. *The Guardian, 16 April 2001*
>
> This is where the dark side of the net comes in handy. If you are (say) a Home Secretary who seeks draconian powers to control the net, your best strategy is to scare the citizenry by exaggerating the risks from criminals and paedophiles to justify those

> powers. Since nobody knows the extent of criminal use of the network, you are unlikely to be challenged on empirical grounds. Blunt assertions from policemen and spooks are all you need. This was how the Regulation of Investigatory Powers Act was pushed through - giving MI5 access to every digital packet flowing through a British ISP's servers. *The Observer 13 May 2001*

The press may also be motivated to debunk myths as part of an exposé on industry practices:

> The seriousness with which we should treat reports predicting the apocalyptic threat of a new and virulent strain of computer virus is not enhanced when, more than occasionally, we can detect that behind the dire warnings lies the clear hand of a company selling just the anti-virus package we need to deal with it. *The Times, 18 August 1995*

A final major category of myth debunking and panic dampening can occur when the press, albeit rarely, give hackers or ex-hackers a voice:

> As editor and publisher of 2600: The Hacker Quarterly, Mr Goldstein feels he has an important role to play. He wants the public to get a more balanced view of what hackers really do, in the face of media representations classifying arrested hackers as computer terrorists...
>
> It is this sort of behaviour that gets computer hackers such a bad name, though they generally tend to denounce these types of activities. *The Independent, 17 July 1995*
>
> Ex-hacker and editor of Hack-Tic magazine Rop Gonggrijp claims the vilification of hackers is just the security industry scaremongering in an attempt to justify its own existence. *The Guardian, 22 May 1997*

Having dealt with the significant cases where the press acts to dampen panic about cyberterrorism, press claims are otherwise diverse and the majority of articles aim to sensitise the public and sensationalise the issues. In common with other sources, the press tends to focus on stories about cybercrime, linking it with terrorism in various ways in order to achieve a degree of excitement not otherwise merited. In terms of symbolism, the hacker, his supposed links with terrorism and his tools, chiefly the Internet, attract special attention.

To underscore the concern felt about cyberterrorism, security threats on the one hand and vulnerabilities on the other are highlighted time and again. Claims often relate to the vulnerability of key systems, providing a locus for the cyberterrorist threat to society.

> [R]eporters, supported by computer experts, discovered that some of BT's classified information had been extracted and placed on the Internet... The world could view some of Britain's most closely-guarded secrets...
>
> Among the downloaded information ... were the locations of radar command posts, Nato fuel depots, tactical air control centres and missile sites, private numbers for members of the Royal Family, secret Bank of England numbers and MI6's training centre. *The Independent, 15 November 1995*

> The most dangerous feature of the new viruses is that many are triggered simply by checking an e-mail in-box. Even if a user does not click on the infected e-mail, let alone open an attachment, the virus will cause huge damage and send itself to every other address in the computer's e-mail software. *The Observer, 7 May 2000*
>
> The United States... has given warning of the importance of protecting its most vulnerable systems from the threat of cyber terrorism. *The Times, 20 November 1999*

Having established cause for concern, the claims move inevitably to the deviants deemed to cause it. Hackers are translated into terrorists. Basic computer-related crime is morphed into 'cyberterrorism', and a simple process of association is the most common mechanism used by the press to achieve this. In many cases, the offenders are termed 'cyberterrorists' explicitly:

> The government has been holding a secret investigation into attacks by cyber terrorists on the City of London for more than two years. *The Sunday Times, 9 June 1996*

This case involved blackmailers who simply threatened to compromise computer systems unless substantial payments were made. There were no genuine connections to terrorist organisations, yet once the word 'terrorists' is mentioned, the association is made. In other cases, the term 'cyberterrorist' is associated with hacker activity, rather than calling hackers 'cyberterrorists' outright:

> So many hackers are using the Internet to try to break into sensitive American military and civil systems that the United States government is about to create an expert team to counter "cyber-terrorism". *The Independent, 7 June 1996*

In the final type of association, hackers and terrorists are simply associated in the same sentence, leaving the impression that they are connected:

> Our species, though, is emotionally driven - and thus flawed. Terrorists and hackers share the warped desire to achieve fulfilment through destruction. *The Business, 15 August 2004*
>
> Millions of people risk having the personal information stored in their mobile phones stolen by a hi-tech electronic eavesdropping device, experts warned yesterday. It would enable paedophiles, terrorists and industrial spies to hack into handsets without the victims even realising. *Daily Mail, 15 April 2004*

As well as providing evidence of the specific rhetorical mechanism of association, these are all examples of the sensationalism which is the key feature of press claims about cyberterrorism. Other examples are varied, sometimes referring to science fiction:

> Imagine the nightmare scenario. Like the movie WarGames, computer buffs hack into - and then take over - the systems controlling defence and economic secrets of every nation in the world. Fantastic? Impossible? We can reveal today that it has happened. *Mail on Sunday, 14 February 1993*

Still other stories portray the actions of hackers in a bizarrely overblown manner, such as this report from the first Gulf War in which some young hackers hacked a European weather computer several weeks before Operation Desert Storm:

> The Allies' success in the Gulf War was put in danger because of three British computer hackers. Plans for Operation Desert Storm had to be dramatically altered after the trio scrambled data in the massive computer which gave General Norman Schwarzkopf vital weather intelligence in advance of the attack on Iraq. The group, operating separately from their bedrooms in the North of England, inadvertently jeopardised - almost fatally - the international effort against Saddam Hussein, putting thousands of servicemen's lives at risk...
>
> Scientists ... at first suspected terrorists or a foreign power had infiltrated their computer when things started to go drastically wrong with the Cray's calculations. *Mail on Sunday, 21 March 1993*

Gross exaggeration is also used to give a story high impact. The following was included in a report that the US government was about to approve the use by its intelligence agencies of certain covert intelligence-gathering techniques which had previously only been allowed with specific presidential approval:

> Since the end of the cold war, a new breed of computer-literate terrorist and organised criminal has emerged. Every terrorist organisation has an array of personal computers and drug barons are investing millions of dollars each year to upgrade computer systems that keep track of their operations. *The Sunday Times, 27 October 1996*

A significant variation on the sensationalisation theme of claims-making is 'prediction'. Here, a piece of information is given and then extrapolated into a 'what if' scenario, termed above the 'future threat scenario'. This is a powerful mechanism used by all claims-makers, and the press are no different:

> Authorities fear terrorist groups could use similar attacks to disrupt rescue attempts after a major atrocity. Terrorists could even black out the electricity network using viruses, or attack air-traffic control systems. *Mail on Sunday, 16 May 2004*
>
> Renegade computer programmers have developed dozens of 'superviruses' that each have the capability to inflict massive damage on global computer systems. The new viruses have many times the destructive power of the 'love bug' which wreaked havoc last week, and there are fears that criminals and terrorists could use them to blackmail governments and private institutions. *The Observer, 7 May 2000*

Summary

The press has a significant role in attenuating the rhetoric of moral panic, exposing the ulterior motives of other claims-makers or giving voice to those who seek to debunk myths surrounding cyberterrorism. This aside, the press underscore generalised concern by highlighting time and again the security vulnerabilities in computer systems, which constitute the locus of the threat to society. Other claims made by the press are many and varied, but always sensational. What draws them together is the rhetorical mechanisms used to get these points across. Sensationalisation has a number of facets, the most significant of which are the future threat scenario, association and exaggeration.

This chapter has analysed the general reporting patterns exhibited by the UK national press in all reports where hacking and terrorism are associated in some respect. Further, it has presented evidence relating to press activity in each of its three main rôles: agenda-setting, image transmission and claims-making. The next chapter will consider the substance of claims made by the other major claims-makers in the cyberterrorism narrative.

CHAPTER 6

FINDINGS: CONCERN, CONSENSUS AND THE CLAIMS-MAKERS

1. INTRODUCTION: CONCERN AND CONSENSUS

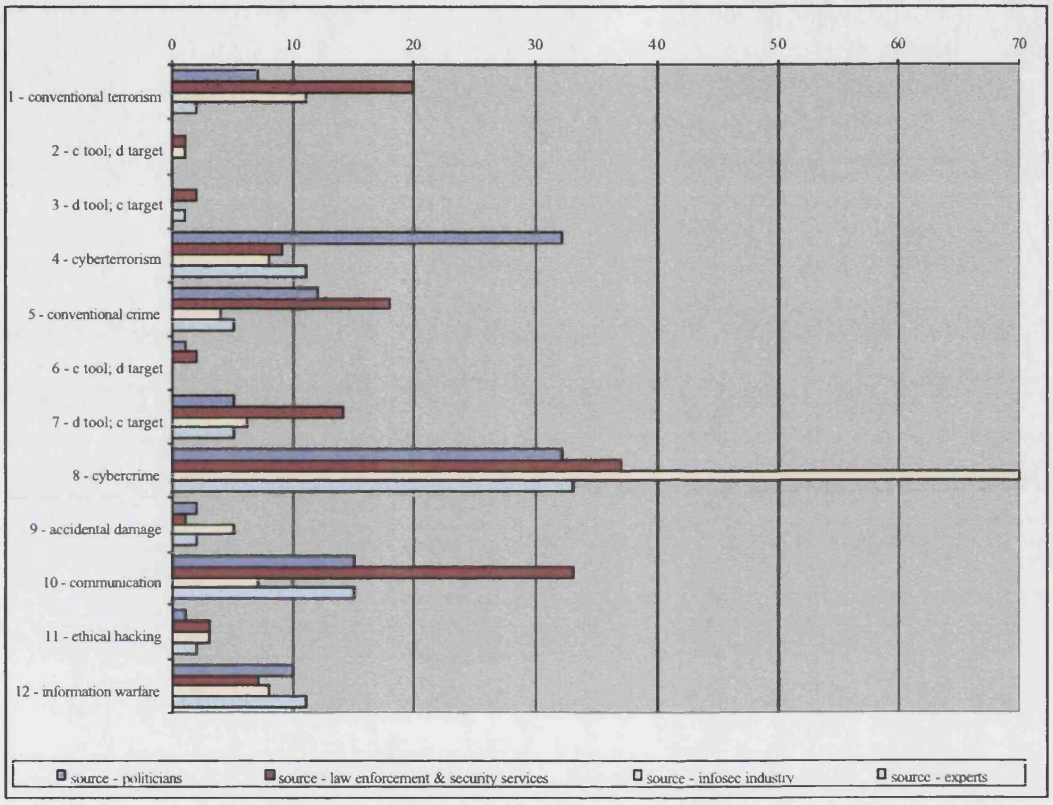
This chapter will deal with three of the six elements of the attributional model of moral panic as modified by Critcher (2003: 151): concern, consensus and claims-makers. Although these elements are distinct, evidentially they are practically impossible to separate. Concern is evidenced by the existence of a prevailing discourse of risk which, although contested, is largely dominant. Claims-makers engage in the discourse, identifying certain behaviour which is ultimately labelled and defined as deviant. Consensus is really a question of the degree to which the prevailing discourse can be said to be dominant and, in the most extreme cases, exclusive. When considering concern and consensus, evidence of one is most often pertinent to the other, so dealing with them both together avoids undue repetition.

The major claims-makers in the discourse on cyberterrorism were identified in Chapter 5 as being those with the most powerful representation in the press: politicians, law enforcement, the information security industry and other 'experts', having either inherent or attributed expertise on the problem situation and possible solutions. The press has been identified as a claims-maker in its own right and those claims were dealt with in Chapter 5. The deviant group itself will be dealt with in Chapter 7.

The analysis in this chapter is organised according to the claims made by the major claims-makers. Before examining these, however, it is convenient to present certain aggregate data so that they can be referred to in later sections. The data presented below represent the number of times a given code was applied to a piece of text from the corpus. Figures 9, 10 and 12 represent the number of cases where two codes have been applied to the same piece of text. For example, Figure 9 shows that there are 70 separate occasions in the corpus where the information security industry is the source of a reference to cybercrime. In other words, each of 70 sections of text was coded with at least two codes: 'source – information security industry' and '8 – cybercrime'.

First, a very general overview of the data presented in Figures 9 to 12. The details will be discussed later in this chapter under headings relating to the main claims-makers in the dialogue on cyberterrorism.

Figure 9 **Frequency distributions of claims-makers' references to behaviour categories**



The frequencies with which each of these groups refers to the different categories of behaviour identified in this study (Figure 9) gives a measure of the types of behaviour which each group of actors considers significant and worthy of concern. The code for type of behaviour is attributed according to an objective assessment by the researcher of what behaviour is being described as opposed to the label attributed to the behaviour by the claims-maker. For example, where a hack attack is described but is labelled by the claims-maker as 'cyberterrorism', the code attributed is '8 – cybercrime' and not '4 – cyberterrorism'.

The striking feature of this dataset, drawn from press articles in which hacking and terrorism are associated, is that cybercrime is overwhelmingly the behaviour category most likely to cause concern overall and it tops the list of concerns for each claims-making group. Members of the information security industry are those most likely to express this concern in the press. Although the term 'cyberterrorism' may be used

widely to refer to all sorts of behaviour, an analysis of the frequency with which claims-makers discuss genuine terrorist cyber-attack, that is 'cyberterrorism' in the sense adopted by this study, shows that frequency to be relatively low. Politicians demonstrate the most concern about cyberterrorism, with three times more reports than any other claims-maker. They are, therefore, by far the most likely to be making claims about the risks from cyberterrorism.

Figure 10 **Recurring themes referred to by different claims-makers**

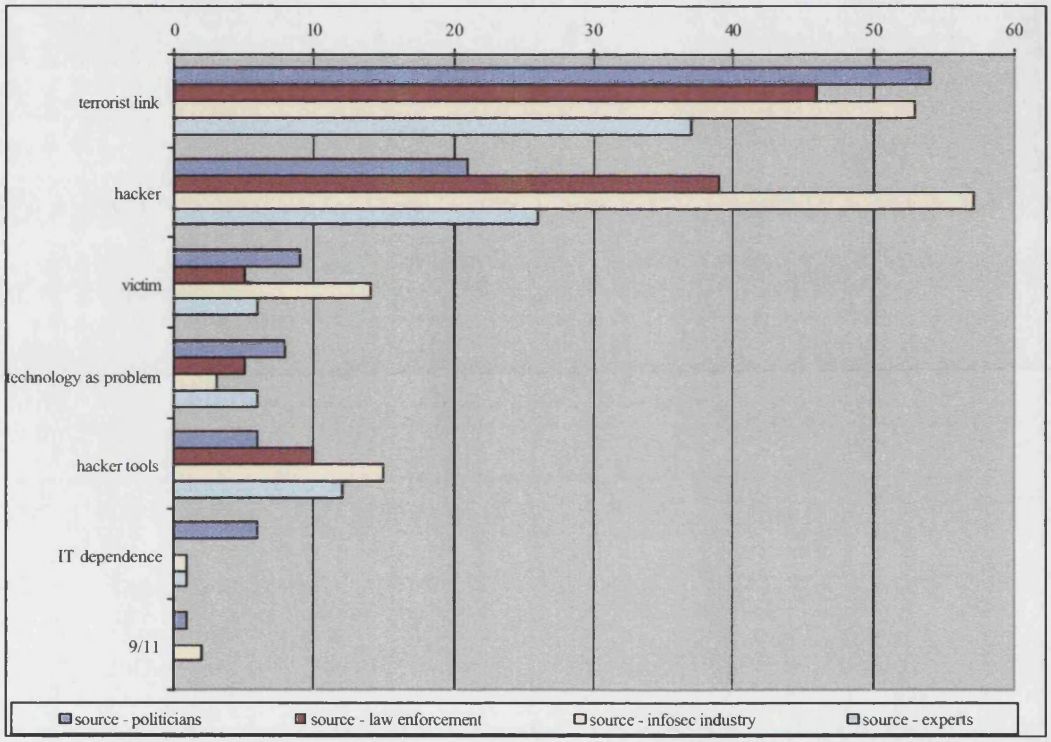


Figure 10 provides an indication of the targets of each group's rhetoric, presenting the frequencies with which each group refers to a number of recurring themes. The relationship between hackers and terrorism is the theme most often exploited in the corpus, with the theme of hackers being very popular also. Such references to risks from the deviant group and their mode of deviance are far more common than references to their victims, the technological threat (technology viewed as problem; hacker tools, such as viruses and use of the Internet) or perceived vulnerabilities (IT dependence). It is also striking that the terrorist attacks of 9/11 in New York (and 7/7 in London, which barely featured in the findings) actually played a very low-key rôle in the presentation of concerns about cyberterrorism by the various claims-makers.

Figure 11 **Frequency distributions for use of specific rhetorical mechanisms found to be significant in the corpus**

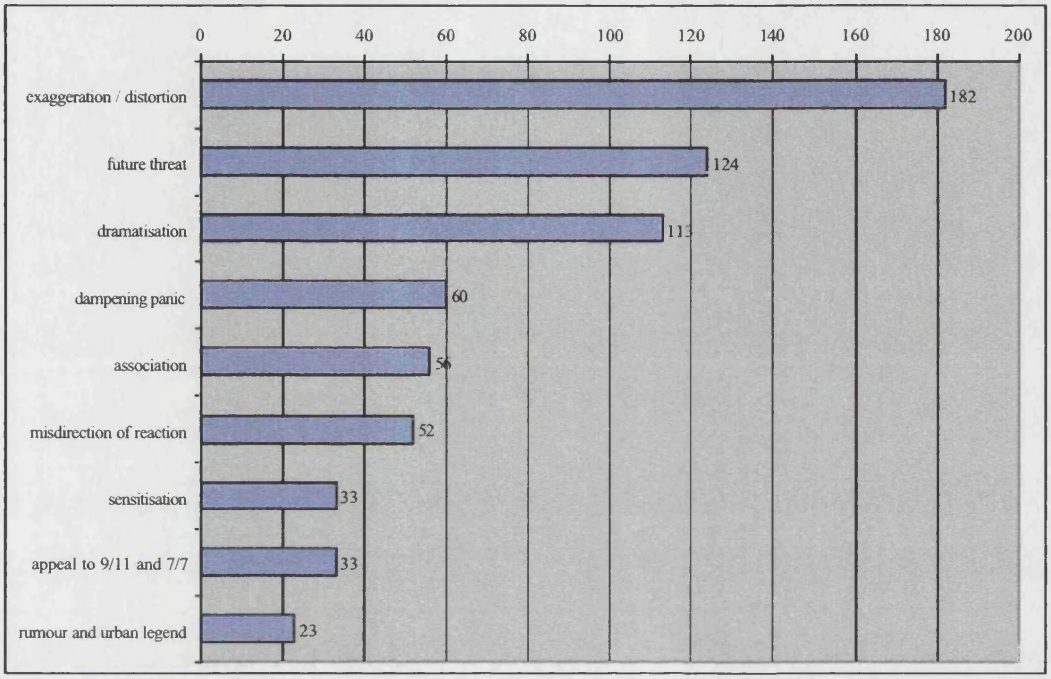
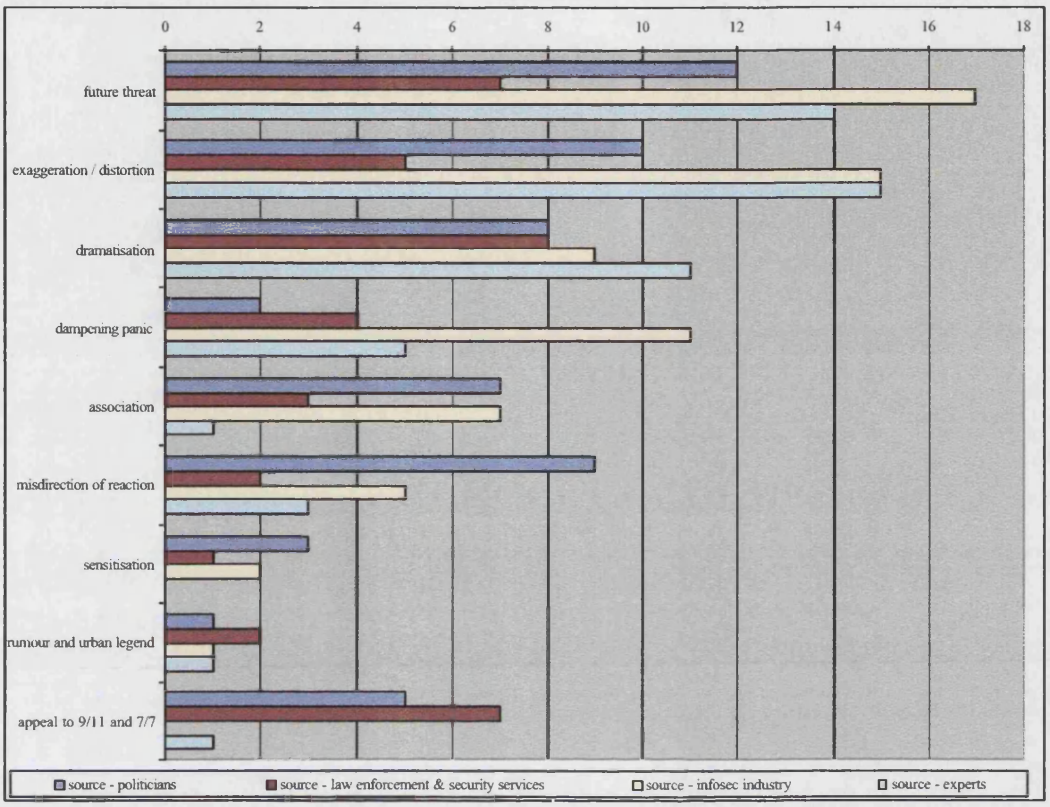


Figure 11 sets out the different types of rhetorical mechanism which were found to be significant in this study in relation to cyberterrorism and shows which were the most frequently used overall. Claims-makers most often resorted to exaggeration or distortion of facts, but also relied heavily on prediction, more specifically what has been termed the 'future threat scenario', and dramatisation, the better to appeal to the imaginations of a readership. It is also worthy of note that there is a significant level of panic-dampening activity amongst claims-makers, who assert that the cyber-disaster claims are overblown and lead to a misdirection of public concern. Once again, it is apparent from the data that the events of 9/11 and 7/7 were used relatively little as a rhetorical mechanism for those making claims about cyberterrorism.

Figure 12 sets out the frequencies with which the four main claims-makers in the cyberterrorism debate use the most prominent rhetorical mechanisms, giving an overview of their respective rhetorical approaches to the subject of cyberterrorism. Note that, if Figure 11 gives frequencies of use of these mechanisms for the corpus as a whole, Figure 12 gives frequencies only for their use by four claims-making groups, thus the sum of the frequencies for each mechanism in Figure 12 falls short of the total frequencies in Figure 11.

Figure 12 **Frequency distributions of rhetorical mechanisms used by claims-makers**



These data are relatively complex and will be discussed in more detail below, however, three points are worthy of mention here. The information security industry, for example, are strong on future threat scenarios, exaggeration and distortion, yet they are also those most likely to debunk overblown claims made by other claims-makers (panic dampening). Politicians are those most likely to misdirect the public reaction, urging the focus of concern in one direction when it might more appropriately be directed in another. Where appeals have been made to the events of 9/11 and 7/7 in order to promote concern about cyberterrorism, these appeals have been made by politicians and law enforcers.

We will now consider, in turn, four categories of claims-maker which have emerged as important from the corpus of data: politicians, law enforcement and security services, the information security industry and other 'experts'.

2. POLITICIANS

Analysis of the quantitative data set out in Figures 9-12 provides an overview of the rôle of politicians in the cyberterrorism debate. As Figure 9 demonstrates, politicians are the most influential claims-makers, with press reports of them referring specifically to cyberterrorism being three times more frequent than the next most influential claims-

maker. Figure 9 also shows that it is just as likely that politicians will be referring to cybercrime but, because cybercrime is linked with terrorism in all of these press reports, there is usually a terrorist angle to these references. This quantitative data supports the qualitative finding elaborated below, that politicians are often guilty of confounding the issue of cybercrime with cyberterrorism, labelling ordinary criminal behaviour as terrorist or simply merging the two together. Figure 10 sheds light on this by showing that, more than any other claims-maker, politicians emphasise the terrorist link, that is, the link between terrorism and hacking or technology or both. In fact, for politicians, this recurring theme is far more significant than other themes which occur in the press, such as 'hackers' and 'victims'.

When making claims about cyberterrorism, politicians use a variety of rhetorical mechanisms (Figure 12) the most important of which is the future threat scenario. They are often found to exaggerate or distort facts or scenarios in order to achieve impact. Dramatisation through scenario building is a popular mechanism for emphasising a point. Politicians are also more guilty than other claims-makers of misdirecting the reaction to an episode. Most often, this takes the form of claiming that certain deviant groups, usually hackers or terrorists, are likely to pose a grave threat to security in certain specified ways when there is little or no evidence to this effect. Occasionally, real events are blamed on hackers or terrorists when, in fact, they had nothing to do with it. Finally, politicians also employ the mechanism of association, described in Chapter 5, whereby hackers and terrorism are mentioned together in such a way as to imply an association between the two.

This quantitative evidence can be backed up with qualitative evidence from the corpus. Although this is predominantly a UK study, it is clear that the politics of cyberterrorism cross national boundaries and the prominence of the US political perspective is apparent in the UK press reports. There is clear evidence that, where the US leads, the UK often follows. The bulk of political discourse, national and international, on the issue of cyberterrorism commences with the findings of a presidential commission set up by the Clinton administration, released in the last quarter of 1997. The Commission on Critical Infrastructure Protection recommended a national strategy for protecting and assuring CNI from physical and cyber threats. The ensuing press reports focussed on claims about the real and growing threat from cyberterrorism, the calls for increased spending on computer security and the need for new government posts to coordinate the response. Although this is predominantly a UK study, it is clear that the politics of

cyberterrorism cross national boundaries and the prominence of the US political perspective is apparent in the UK press reports. There is clear evidence that, where the US leads, the UK sometimes follows. The bulk of political discourse, national and international, on the issue of cyberterrorism commences with the findings of a presidential commission set up by the Clinton administration, released in the last quarter of 1997. The Commission on Critical Infrastructure Protection recommended a national strategy for protecting and assuring CNI from physical and cyber threats. The ensuing press reports focussed on claims about the real and growing threat from cyberterrorism, the calls for increased spending on computer security and the need for new government posts to coordinate the response. *The Independent* gives a sense of the surprise felt by many American citizens at this apparently new vulnerability:

> For a country relatively free from terrorist attack inside its borders, news of this vulnerability comes as a shock. The more computerised, the more technologically sophisticated they become, they are being told, the more vulnerable they are to cyber-terrorism. *The Independent, 22 October 1997*

Following publication of the report, US politicians gave their view on vulnerabilities to an increasingly apprehensive audience:

> Consider this litany of woe. From former National Security Agency director John McConnell: "We're more vulnerable than any other nation on Earth." ... Or former US Deputy Attorney General Jamie Gorelick, speaking at a Senate hearing: "We will have a cyber equivalent of Pearl Harbor at some point, and we do not want to wait for that wake-up call." And, Gorelick added, I-War "can disable or disrupt the provision of services just as readily – if not more than – a well-placed bomb." *The Independent, 22 February 1998*

Finally, President Clinton used his trademark, elegant simplicity to press the point home:

> "As we approach the 21st century, our foes have extended the fields of battle from physical space to cyberspace... They may attempt cyber-attacks against our critical military systems and our economic base. We will launch a comprehensive plan to detect, deter and defend against attacks on our critical infrastructures." *The Times, 27 May 1998*

Following closely on these remarks, a mock 'info-war' was set up between the US and the UK in order to test each other's vulnerabilities to cyberterrorism and information warfare.

> Britain and America are about to go into battle in cyberspace. Staging a secret "information warfare" exercise in London later this month, the two governments will test their defences against the futuristic threat of terrorists using computers to bring the West to its knees...
>
> ...the exercises follow recent warnings from President Bill Clinton about the need for vigilance. Tomorrow's enemy, he believes, will know better than to wage all-out war against America and her allies as Iraq's Saddam Hussein did in 1991.

> Instead, small terrorist organisations or tinpot dictators might resort to biological weapons or information warfare, in which computer systems controlling airports, hospitals, traffic lights, banks and even nuclear weapons could be disabled, spreading more chaos than any conventional terrorist attack. *Sunday Times, 7 June 1998*

The potential for devastation of the CNI, including air traffic control, hospitals, defence systems and nuclear plants, and the chaotic, deadly consequences of such an attack has become a pervasive theme in the cyberterrorism discourse. Following this Anglo-American exercise, the British Home Secretary picked up the rhetorical baton, making the transfer from US to UK complete.

> The Home Secretary, Jack Straw, has taken on responsibility for protecting Britain's computers, including those in banking and airlines.
>
> His advisers have warned that as Britain becomes more reliant on computers, vital Government systems, including those in the health service, air traffic control and defence, are becoming more and more vulnerable to malicious attack. *The Independent, 7 February 1999*

This sequence of events illustrates the primary rôle of politicians in the cyberterrorism dialogue: sensitisation and fostering concern (Section 2.1). In quantitative terms, these are by far the most common activities found in the corpus and the focus tends to be on the lack of security and, therefore, vulnerability in given situations. The next most common activity for politicians is making specific claims about cyberterrorism, what might happen and who is responsible (Section 2.2). This can be characterised as an attempt to forge a consensus in the generalised belief system about what the problem is and what must be done. Each of these three major activities will be examined in more detail below.

2.1 Fostering concern

Highlighting existing vulnerabilities is the main tool used to foster concern. These vulnerabilities are often not empirically demonstrated, but rather products of the rhetoric of fear. Politicians are the key actors when it comes to emphasising electronic vulnerabilities and the threats from terrorism:

> Pentagon chief Donald Rumsfeld admitted recently that while "we are safer today from the threat of massive nuclear war than at any point since the dawn of the atomic age, we are more vulnerable now to the suitcase bomb and the cyber-terrorist". *The Guardian, 2 May 2001*

British ministers have not shied away from blunt assertions of impending disaster for the CNI, despite a lack of evidence in support of those assertions:

> Computer hacking could now cripple Britain more quickly than a military strike or terrorist campaign, Robin Cook, the Foreign Secretary, told the Commons last night. He said that the electronic technology controlling essential services such as water, power and transport had become a leading target for terrorists and other groups who wanted to disrupt the life of the nation. *The Daily Telegraph, 30 March 2001*

The economic well-being of the nation is also at stake, it seems, although the claims are not supported with any evidence:

> E-commerce minister Douglas Alexander yesterday ordered internet security to be stepped up. He warned web experts from MI5, the MoD and GCHQ that increased vigilance was needed as terrorists could inflict major economic damage by bankrolling rogue computer hackers and infecting systems with a lethal virus. *The Mirror, 27 September 2001*

The presentation of the worst-case scenario has become characteristic of political assessment of an electronic threat. Often, claims about vulnerabilities are combined with claims about the ease with which they can be exploited, as in this example where US defence systems are tested using 'hacker tools' which can be downloaded from the Internet by anyone:

> Robert Ayers, chief of the Information Warfare Division at the US Deputy Directorate for Operations, conducted an officially sponsored four-year attempt to break in to Department of Defense computers.
>
> Using hacker tools downloaded from the Internet, and only attacking systems when invited to do so, his team succeeded in taking control of the network in 88 per cent of attacks. Of those, 95 per cent went undetected. "I believe between a quarter and a half a million successful intrusions occurred in the US military computers in 1995," says Ayers. "That's a scary number." *The Guardian, 22 May 1997*

What starts in the US is sometimes followed in the UK, and this kind of systems testing is an example:

> Britain's vulnerability to information warfare has recently been the subject of scrutiny in the form of a 'threat assessment' co-ordinated through the Cabinet Office...

Although the results of this assessment were reassuring, government spokesmen still employed the 'just because it hasn't happened yet doesn't mean it's not going to...' argument, a variant of the future threat scenario:

> ...The outcome, so far as it went, was reassuring: they found 'no sign of any systematic attack'. But those involved acknowledge that complacency would be misplaced. 'There may be no evidence of any foreign government with hostile intent, but everyone can see the threat coming,'...
>
> ... the complexity of the technologies involved ... offer the hacker a challenge and the terrorist an opportunity. *The Guardian, 22 May 1997*

Reassurance is notably absent from the official presentation of vulnerabilities due to cyberterrorism and related threats. Politicians are active in highlighting the potential dangers which exist even in our own homes. Under the headline "*Electronic Pearl Harbor: Should we be more worried about terrorists using digital weapons rather than chemical and biological attacks?*" Erkki Liikanen, European Commissioner for the Information Society, claims:

> "More households are signing up for broadband internet services because they offer faster access and an "always on" connection. This, of course, increases the vulnerability of systems and multiplies the probability of some sort of cyber-attack..." *The Guardian, 20 February 2003*

It is the networked and interdependent nature of modern information systems that motivates politicians' attempts to shock individuals and companies into taking the cyber threat seriously:

> Schmidt [advisor to President Bush on cybercrime] pointed to evidence discovered by US investigators on computers found in Afghanistan that suggested Al Qaeda operatives had been planning to disrupt Western power, telecoms and water supplies by hacking into computer systems.
>
> "There is only so much governments can do on their own," says Schmidt. "Almost 85 per cent of the computer systems on which society depends are in private hands, so we need a partnership approach to the problem. Everyone has to do their share to secure their little piece of cyberspace." *Sunday Express, 24 October 2002*

When it comes to society's electronic vulnerabilities, the politicians leave us in no doubt that, first, there is a clear and present danger and, second, that each citizen should be concerned and must play their part in securing the nation.

2.2 Politicians as claims-makers

> ... Republican Senator John Warner told the committee in Washington the nation 'would be unforgiving' if a terrorist attack occurred and it was later determined that the government hadn't done enough to stop it. *The Guardian, 18 March 1999*

It is timely to remember that a primary duty of any government is to promote national security by all reasonable means. Senator Warner's remarks remind us of this, together with the fact that a government also has a duty to look forwards, to try to read the path of future events and, where necessary, to take precautionary measures against possible mishap. As events a mere two years after Warner's address tragically demonstrated, atrocities can and do occur in the real world, despite the best defensive preparations. Yet there should be caution at the other end of the scale. With frequent calls for action, new laws and new police powers in the name of countering threats to national security, the problem is how to decide what measures are appropriate to the particular risk. Some commentators have argued that politicians are not necessarily reliable arbiters in this respect:

> ... politicians cannot be trusted to decide whether a person should be deprived of his liberty. The government hates judges because they cannot be relied on to do what it wants. That is precisely why judges alone should decide. Ministers do not weigh evidence. They measure political risk. There is little in detaining too many [terrorist suspects without trial], but a lot in deciding to release. Political risk should not be confused with threat to the nation. Politicians have a vested interest in talking up threat levels. They use a circular argument. The threat justifies the detentions and the detentions offer "proof" of the threat. *Sunday Times, 30 January 2005*

The question is: how far is society prepared to go to defend itself from attack? The answer depends on your view of the future, which in turn depends on the way you use existing information to extrapolate predictions: a good formulation of the future threat scenario.

Figure 12 highlights the fact that the rhetorical mechanism most used by politicians in relation to cyberterrorism is indeed the future threat scenario. To recap, the argument runs along these lines: an event or state of affairs is specified and this is used as evidence that electronic catastrophe is inevitable and, often, imminent. The specified event or state of affairs used as evidence in the future threat scenario changes over time and examples have included: society's increasing reliance on computers and corresponding vulnerability; 9/11; and the second Gulf War. These events and the claims which they generated are examined in more detail below.

(a) Reliance on computers means inevitable cyber-attack

The increasing reliance of developed Western economies on computerised systems throws up vulnerabilities of an order not previously experienced. Politicians consider this a cause for deep concern and frequently attempt to engender this concern in society at large. In his famous 2001 speech in the House of Commons, Robin Cook, then Foreign Secretary, highlighted the vulnerabilities caused by reliance on computers and used this as a springboard for his ultimate argument: that computer attack is potentially more devastating than a conventional military attack.

> "The revolution in communications technology is creating new opportunities on an exponential scale. This week, 360,000 e-mails will be sent in Britain every second, a fifth more than in January and twice as many as last June.
>
> "Computers now manage most of our critical national infrastructure, but with these new opportunities there also comes the risk of new threats.
>
> "A computer-based attack could cripple the nation more quickly than a military strike." *Daily Telegraph, 30 March 2001*

The government's security advisors cited increasing security in other areas as the main reason for the growing focus on electronic attacks. Simply put, as conventional targets are better protected, electronic targets become an easier option for those wishing to damage British interests.

> Sir David, the Government's security and intelligence co-ordinator, outlined how the terrorist threat might develop in the next five years. ... "We must expect there will be a shift to softer targets including economic targets, in response to our enhanced security."
>
> ... "We should expect attacks on our information infrastructure, some from terrorist-inspired motives as well as criminal."

> Officials are concerned that terrorists will target both public and private sector computers. The cyber-terrorists would disrupt communications, including the banking and benefit computer networks.
>
> Another strategy would be to hack into defence computer systems or systems operating sewage and water supplies. A cyber attack could halt electricity grids, cause air traffic control systems to fail and disrupt the credit-card network. *The Times, 23 March 2004*

Disaster scenarios such as electricity failure and air traffic chaos are now well rehearsed in discourse on cyberterrorism and will be familiar to anyone who reads a newspaper on a regular basis.

(b) Speculation on al-Qaeda

Of all the events which could have prompted widespread concern over the threats from cyberterrorism, the attacks of 11 September 2001 are the most obvious. There was widespread newspaper coverage of this concern, ranging from speculation as to what al-Qaeda might or could do, to claims as to what al-Qaeda were actually doing.

As with the case of the power failures in North America on 14 August 2003, basic, criminal activity such as spreading viruses has been blamed on 'cyberterrorists', a good illustration of how cybercrime and cyberterrorism are often confounded. Similarly, after 9/11 some were quick to attribute virus activity to al-Qaeda even though there was no real evidence of any terrorist motive:

> Security chiefs fear that followers of Osama Bin Laden have turned to cyber terrorism in a plot to paralyse Western governments.
>
> Mystery hackers have spread a highly destructive virus through the European Parliament's e-mail network. Now there are fears it could be passed on to government systems all over the world.
>
> One Euro source said: "This could be the work of al-Qaida terrorists." *The People, 16 June 2002*

This virus incident was followed later that month by more fears specific to al-Qaeda. On 28 June 2002 *The Guardian* published two separate, but almost identical, stories with eye-catching headlines: "*US fears al-Qaida hackers will hit vital computer networks*" and "*Al-Qaida planning cyber-attacks*".

> The al-Qaida terrorist network has been making preparations for potentially devastating attacks on America by hacking into computer networks to look for ways to disrupt electricity and telephone systems, dams and nuclear power stations, it was claimed yesterday.
>
> Government officials said the terrorist group appeared to be far more sophisticated than initially thought in its use of the internet as a weapon to disrupt America's web-based economy and cause potentially catastrophic physical damage by opening dam floodgates or blacking out air traffic control systems. *The Guardian, 28 June 2002*

These claims are unequivocal, yet the only evidence offered in support relates to al Qaeda suspects browsing websites offering hacking tips and others not even identified

as al Qaeda affiliates "studying US computer systems" connected with the CNI. Nevertheless, a Presidential adviser is motivated to claim:

> "We were underestimating the amount of attention (al-Qaida was) paying to the internet," Roger Cressey, the chief of staff of the White House critical infrastructure protection board, told the Post.
>
> "Al-Qaida spent more time mapping our vulnerabilities in cyberspace than we previously thought. The question is a question of when, not if." *Sunday Express, 24 October 2002*

There is a strong assertion of the future threat scenario here. Although Cressey does not explicitly state what he is expecting, the context makes it clear that he considers a cyberterrorist attack inevitable.

Political rhetoric has also dealt with the motivational principles imputed to al-Qaeda. In the passage below, two rather strange claims are made. First, that the spectacular conventional attacks on 11 September 2001 somehow crystallise the threat from *cyber*terrorism. Second, that it is not possible to damage the economic infrastructure of the West through conventional attacks, therefore cyberterrorism will become the weapon of choice. For good measure, a reference to the vulnerability of the emergency telecommunications system is brought in at the end to continue the CNI theme.

> But it's the events of September 11 2001 that have turned cyber-terrorism from a theoretical threat into a very real one. The warning signs are there for all of us to see in al-Qaida's public statements, says Richard Clarke, chairman of the president's critical infrastructure board. ... His argument is quite simple: before September 11, al-Qaida tended to talk about taking human lives – killing as many people as possible. But afterwards its rhetoric shifted towards threats against the economic infrastructure of the west. This is too dispersed and diverse to bring down with bombs, he argues, but it could do a lot of damage in cyberspace...
>
> ... "Now, if you're a terrorist, the first thing you might want to do before an attack is take down the 911 system," says Clarke. *The Guardian, 20 February 2003*

A major problem with these claims is that it is by no means apparent that a ramping up of conventional attacks heralds the arrival of cyber attacks. It may certainly justify the speculation that further spectacular *conventional* atrocities may occur elsewhere in the world, and such speculation was proved horribly prescient by the subsequent bombings in Madrid, London, Turkey and Egypt. But the idea that al-Qaeda has moved on from the conventional to the cyber attack is simply not borne out by the available evidence presented to the public and reported in the press. Assertions that the only way to damage a Western economy significantly is by cyber-attack are not easily credible. Consider, for example, the damage to lucrative tourist industries caused by fears of further bombings; the prohibitive costs of clearing up and making good after a major incident such as occurred in London; the revenue lost by businesses due to closure of

offices and staff being unable or unwilling to turn up for work. It is often the case that the 'economy' is identified with the stock exchange in any given country. Yet, intuitively, how much easier would it be to bomb a physical stock exchange than to penetrate its distributed information systems and damage them electronically? Even allowing for disaster recovery provisions, the economic damage from a bomb in these circumstances would surely resound throughout the world as other exchanges felt themselves vulnerable.

(c) Speculation on Gulf War II

The second Gulf War was a further event used to support claims that electronic catastrophe is inevitable and imminent. Once again, the future threat scenario is used to build and maintain levels of concern. The warnings started before the war:

> Terrorist groups may try to infiltrate the computer systems of some of Britain's biggest companies, government departments and emergency services if a war is launched against Iraq, the Home Office has cautioned. *The Times, 20 February 2003*

We now know that Islamic extremists did not resort to cyber-attack: they remained committed to the gun and the suicide bomb.

> The war in Iraq was supposed to dramatically raise the likelihood of a major cyberterrorist attack against the US and its allies. Some even predicted a "digital Pearl Harbor", an electronic assault that could have shut down power plants, crippled the banking system, or disabled the air traffic control network. ...
>
> Now with the war winding down, fears that Iraq, al-Qaida or even sympathetic hackers in Russia and China would open up a second front in cyberspace have turned out to be completely unfounded, with little or no evidence that either they or anyone else engaged in cyberterrorism. What happened?
>
> Quite simply, the expected attacks just never materialised. *The Guardian, 24 April 2003*

The article went on to explain that neither the US military nor Symantec had detected any significant increase in attacks as a result of the Gulf War. Yet when politicians make predictions which do not materialise, the future threat scenario still holds good. The power of this mechanism is, of course, that it is impossible to refute: there were no attacks this time, but there may be in the future. Such was the case with claims made about the risks of cyberterrorism as a result of the second Gulf War:

> Even if the risk of cyberterrorism during the war was overstated, the threat of a serious attack by a rogue nation or a terrorist group remains very real, according to US government agencies. Recent reports by the FBI and the Department of Homeland Security have outlined the continuing danger of terrorist groups turning to the internet. One particular concern is that cyberterrorism might be timed to coincide with a physical terrorist attack, such as bombing a building while simultaneously disabling the emergency response system, to ensure that the maximum number of lives were lost. *The Guardian, 24 April 2003*

Yet again, the vulnerability of the CNI is emphasised in order to make the future threat seem more immediate and believable, providing something on which the imagination might seize. The following passage provides another example of this technique, as well as employing the asymmetry argument in the attribution of a new rationale for cyber attack: extremists have lost the war and cannot hope to win against the might of the USA in a conventional fight. Therefore, they will resort to the asymmetry of cyber-attack where they can achieve greater purchase.

> [G]iven the recent show of American military superiority in Iraq, cyberterrorism might prove attractive to extremist groups looking for a more level playing field on which to fight. ...
>
> Congressman Andrews predicts that if the US does not find a way to make its critical infrastructure more secure, there will be a "significant cyberattack within the next five years, whether it is on the 911 emergency response system, the power grid, the banking system or the air traffic control system". *The Guardian, 24 April 2003*

As so often before, this amounts to little more than speculation, and there is no evidence for these assertions other than the fact that the argument seems logical. The message is also expected to sink in through sheer repetition of the vulnerabilities in our CNI.

As noted at the beginning of this section, a government has a duty to look forwards, to try to read the path of future events and, where necessary, to take precautionary measures against possible mishap. The keystone of this process is the way existing information is used to extrapolate predictions. The problem in the context of cyberterrorism is that information is either absent, incorrectly interpreted or entirely fabricated and it follows that the predictions based on this information, or lack of it, are flawed. Nevertheless, these predictions are used as justification for calls for the enhanced social controls which are explored further in Chapter 8.

Summary

Politicians are major claims-makers in the cyberterrorism debate and their views are reported in the press more often than any other. They tend to confound the issues of cybercrime and cyberterrorism, either for political expediency or through lack of rigour. Politicians tend to exaggerate and distort the facts, but the most important rhetorical mechanism is the future threat scenario: an event or state of affairs is specified and this is used as evidence that electronic catastrophe is inevitable and, often, imminent. Even if the predicted events do not ultimately come about, politicians are adept at using the ultimate power of the future threat scenario: the impossibility of proving that such a scenario will never take place. If the event did not happen as they predicted, it is

possible to argue that it may still happen, or society may still be vulnerable for different reasons.

3. POLICE AND SECURITY SERVICES

When coding the corpus, the 'security services' variously included intelligence services and, where the context was appropriate, the military. During the coding process, the police and security services were dealt with together since their concerns were most often identical. Nevertheless, there were occasions where a distinction needed to be drawn and, where relevant, this will be made clear. Unless otherwise stated, however, from now on these two groups are referred to collectively as 'law enforcement'. It is recognised that this is a somewhat unorthodox shorthand when used to include intelligence and security functions.

An analysis of the types of activity most frequently referred to by law enforcers reveals that cybercrime is the most important (Figure 9). This is to be expected, since the police are the law enforcers most often quoted in the press and they are usually concerned with the investigation of incidents which have already taken place. By far the most common type of cyber-delinquency reported in the corpus is ordinary cybercrime (Figure 6 in Chapter 5), such as hack attacks and theft of information held on a computer, and it is these offences which are investigated by the police. The second most popular behaviour for discussion is communication. The way criminals and terrorists communicate with each other and run their operations is of prime importance to law enforcers and it is clear that they will be extremely concerned, not only with the method of communication, but also with the substance. Use of the Internet by deviant groups has long been a concern for law enforcers, and this concern will be investigated further below (Section 3.1 (a)).

Other categories of behaviour are much less often discussed by law enforcers. Some attention is given to conventional crime which, bearing in mind that this comes in the context of reports citing both hacking and terrorism, may indicate that law enforcers are more likely than other groups to confound conventional crime with its cyber relatives. A recurring example in the corpus was the case where extortion is attempted using threats to compromise an electronic system. This has been referred to as 'cyberterrorism' but, according to the taxonomy used in this study, it does not even qualify as cybercrime. The only electronic element present is the threatened computer system, but no electronic manoeuvre is ever made. When the codings are analysed more closely, however, it becomes apparent that the police themselves are not generally

confounding conventional crime with cybercrime or cyberterrorism: it is the reporting of these cases in the media which introduces the confusion. Whilst a police officer will have used the word 'extortion' this will be juxtaposed with the word 'cyberterrorist' in the text of the article, leaving the impression of a terrorist link where none was intended by the police (this example from *The Sunday Times, 2 June 1996*). Indeed, the police are commonly meticulous in their characterisation of deviant acts as cybercrime, computer-related crime or terrorism. This is borne out by the fact that law enforcers refer to cyberterrorism infrequently and then only in the abstract since available information suggests they have never had to investigate such an episode.

Finally, law enforcers are those most likely to refer to conventional terrorism and the type of computer-related crime which applies a digital tool to a conventional target. In fact, when the distribution of frequencies with which law enforcers refer to each activity in the taxonomy (Figure 9) are compared with the overall frequency distributions of press reporting of these activities (Figure 6 in Chapter 5), there is a very good fit between the two, and the police are unique amongst claims-makers in this respect. This tends to suggest that they are not focusing unduly on one type of behaviour for rhetorical purposes. It might be said that they 'speak as they find', attaching a reasonably accurate and impartial label to the cases they investigate.

That said, of the various themes which recur in press coverage of cyberterrorism generally, there are two to which law enforcers make reference far more frequently than all others: the theme of hackers and the theme of the terrorist link (Figure 10). When discussing these themes, law enforcers are most likely to use the mechanism of dramatisation in order to emphasise a point (Figure 12). Here, the use of illustrative examples serves to highlight the concerns of law enforcers. Law enforcers are less likely, on the other hand, to employ the rhetorical mechanisms of the future threat scenario, exaggeration and distortion. The qualitative evidence puts this quantitative information into perspective. Perhaps knowing they cannot risk crying wolf too often for fear that the public will ignore their warnings, the police are habitually cautious when making specific claims about future threats. As a result, claims about the threat from hackers and cyberterrorism are seldom made and, even then, are relatively muted and rarely, if ever, sensationalist. Referring to the possibility of cyber-sabotage by temporary workers with an anti-capitalist agenda, the police issued a warning, but qualified it as merely taking precautions:

> 'We are aware that a number of events are being planned for the May bank holiday weekend,' admits a spokesperson from the Metropolitan Police, adding that they are merely taking precautionary measures to avoid a repeat of last year's protest, in which rioters brought terror to the financial district and caused £2 million of damage. *The Guardian, 17 April 2000*

Eliza Manningham-Buller, then director general of MI5, warned a CBI conference that she was concerned UK companies were becoming complacent about an attack because, at that time, the UK had not been targeted for outrages on the scale of 9/11 or the Madrid train bombings. She avoided sensationalism, however, merely urging organisations to engage in the kind of security activity they should in any event be considering in the course of their everyday business:

> "My message is to broaden your thinking about security issues. A narrow definition of corporate security including the threats of crime and fraud, should be widened to include terrorism and threat of electronic attack." *The Independent, 9 November 2004*

3.1 Concerns

This section sets out those concerns law enforcers brought to public attention by means of the press. As availability and use of the Internet became more widespread, it became inevitable that old forms of deviance would be given a new form of expression and that new forms of deviance would become possible. This state of affairs was legitimately a source of concern for the police because it brought with it new challenges for law enforcement. Of course, the existing law could be used in many cases, so that the main challenge for the police was one of resources and expertise in the investigation process, since an understanding of and aptitude in the use of computers and networks was necessary. In some cases, however, there were genuinely acts of deviance which did not appear to be covered by any existing law, and these were generally grouped under the term 'hacking'. In this respect, the police not only lacked the skills and resources for investigation, but also the law had been found wanting. At this time, there was no such thing as a computer crime unit and calls for new legislation came from the Fraud Squad:

> Scotland Yard's fraud squad is backing demands for computer hacking to become a criminal offence. *The Independent, 15 May 1989*

Legislation was duly passed in the form of the Computer Misuse Act 1990, but the challenges arising from lack of skills, resources and organisation remained and, indeed, remain to this day.

(a) Internet as problem

> Detective Superintendent Brian Drew of NCIS said: "Criminals are diversifying. They are using the tools that the Internet provides. Interception of these communications is very difficult." ...

> ... Albert Pacey, director general of NCIS, said that new information technologies and particularly the Internet presented a serious problem.
>
> "A new police beat is emerging," said Mr Pacey, "not that of the streets of our cities but that of the information highways which are creating criminal opportunities that ultimately affect every citizen." *The Guardian, 29 May 1997*

It is axiomatic that one of the greatest hurdles to online policing is the fact that the Internet reduces or removes the significance to the user of geographical boundaries, time, identity and personal resources. Conversely, the importance of these things increases for law enforcers when attempting either to gather intelligence or investigate an offence. Geographical boundaries suddenly become a barrier to investigation because of the territorial nature of the police:

> Acknowledgement of the international scope of computer crime is illustrated by an Interpol working manual that an international police committee ... is issuing to more than 150 countries round the world. The manual is planned as a common vade mecum for the computer investigator so that the FBI man in New York can talk to a counterpart in Hong Kong, Moscow or Nairobi. *The Times, 20 December 1995*

Time is of the essence, since evidence can be erased quickly:

> Detective Inspector John Austen was tired but philosophical. Working on an investigation through the night is one of the penalties of running the police team in Britain dedicated to patrolling the emerging world of the computer criminal.
>
> "We have entered a global village where normal time and geography do not apply.
>
> Because things happen so quickly and briefly we have to act quickly," he said. *The Times, 20 December1995*

Identity becomes all but impossible to establish:

> ... when the authorities intercept anonymous criminal boasts about thefts and acts of sabotage, it's often impossible to tell which crimes really happened, and which were merely imagined. *The Independent, 8 August 1992*
>
> ... the American government, backed by the FBI, is concerned that [encryption] will be used by terrorist organisations to pass instructions and plan bombings or organise riots across the world without the risks involved in physical or telephone contacts. Who needs a "dead letter drop" – open to covert surveillance – when you can encode the information to be picked up anonymously on the Net? *Sunday Times, 3 August 1997*

Users need only limited personal resources to effect a correspondingly large amount of harm, whereas the police need vast resources to conduct their investigations; where one user can perpetrate a crime, many officers are necessary to investigate.

> Britain faces a growing threat of an electronic attack by terrorists linked to al-Qaida that could paralyse key public services, including electricity and water supplies ...
>
> For terrorist groups like al-Qaida with limited resources, it would be "a very attractive method" of attack, that would cause "huge damage", said Stephen Cummings, director of the National Infrastructure Security Coordination Centre. *The Guardian, 12 August 2002*
>
> What delights the protesters – but worries their opponents – is that the internet acts as a magnifying glass for discontent. Individuals using computers can wield power they

vulnerabilities which, if exploited, would lead to catastrophic consequences, nor whether there are cyberterrorists ready and able to exploit them.

The next two sections set out the views of those on either side of this debate.

4.1 Cyberterrorism as threat

In common with other claims-makers in the late 1990s, notably politicians (section 2.2 above), the information security industry voiced concerns that cyberterrorism was a logical next step for terrorist groups, and that the targets would be the economy and the CNI. This was an emerging idea, the public discourse about which was largely triggered by President Clinton's Commission on Critical Infrastructure Protection which published its findings in 1997 (see further section 2.2 above).

> Dr Neil Barrett, an expert on computer hacking and "information warfare" ... predicted that organisations such as the IRA and Animal Liberation Front would soon take advantage of the technology. "It's such an obvious and logical next step, it's something we anticipate," he said. He added that terrorists of the future might use computer viruses to cripple emergency and public services rather than bombs. *The Independent, 29 May 1997*

> Neil Barrett, senior consultant with Bull Information Systems, said terrorists found the Internet an obvious choice for their activities.
>
> "Certainly it is very attractive to them," he said. "Border controls can pick up things like Semtex but they cannot detect computer viruses." Terrorist groups could cause economic damage without the risks they ran in planting bombs. *The Guardian, 29 May 1997*

An obvious next step for terrorists, perhaps, but one which did not materialise in the years that followed. Still, the warnings did not stop and, indeed, gathered force over the years so that the response to claims about the future threat of cyberterrorism grew stronger in proportion to the strengthening conviction of its imminence.

> ...government and private computer experts will be ... look[ing] into the growing possibility of a "cyber-terrorist" attack on what is known as our "critical information infrastructure" – the electronic systems vital for government, armed forces, business, finance, telecommunications, utilities, or emergency services.
>
> There have been warnings from parts of the IT community that terrorists could attempt something like this for at least 10 years, but now governments are taking it much more seriously. *The Guardian, 20 February 2003*

Having predicted a future threat which did not come about, some members of the industry resorted to labelling ordinary criminal and delinquent behaviour 'cyberterrorism'. Thus, the teenager known as 'Mafiaboy', who brought several high-profile websites to their knees, including CNN, Yahoo!, eBay, Amazon and Etrade, became a cyberterrorist. According to the experts, he and his ilk were dangerous and here to stay.

> introduction of compulsory identity cards as an absolutely essential tool in the war against terrorism. *Sunday Express, 16 November 2003*

Certainly, law enforcers are concerned about computer-related crime and terrorism, particularly given the new dynamic introduced with increased use of the Internet, and they are keen that the public should treat information security seriously. Yet law enforcers are also keen that the public should not forget that conventional methods of crime and terrorism are still the bigger threat.

> I am concerned that this connectivity and dependency make us vulnerable to information warfare attacks. While attention is focused on computer-based attacks, we should not forget that key nodes and facilities that house critical systems and handle the flow of digital data can also be attacked with conventional high explosives. *John Deutch, Director of the CIA, from a speech given to the US Senate Governmental Affairs Committee 25 June, reproduced in The Observer, 7 July 1996*
>
> It is not uncommon for terrorist organisations to do business with other forms of organised crime...
>
> But ... there is 'absolutely no suggestion' that terrorists would be involved in hi-tech, multi-million-pound attacks on City firms. 'Why bother with the effort of hi-tech when you can make all the money you need from drug dealing or credit card fraud?' *The Observer, 17 July 2005*

In summary, law enforcers view the Internet with concern, since it is a facilitator of crime and terrorism and they lack the skills and resources to fight on equal terms with the perpetrators. That said, law enforcers retain, on the whole, a balanced outlook and recognise that the main dangers to the public, business and national security remain conventional for the time being. The rhetoric used is rarely inflammatory, and a measured approach to the issue of criminal and terrorist use of the Internet is maintained.

(b) Concerns relating to terrorism

It is interesting to note that the press do not often report law enforcers as being preoccupied with terrorist, as opposed to criminal, use of the Internet until after 9/11. There is concern before this time, but it rarely finds a voice. Prior to 9/11, the most often reported sources of concern over terrorist cyber-attack came from the US law enforcement agencies. Use of the future threat scenario was common, because they were discussing possibilities and openly admitted that no such attack had so far taken place, but the wild exaggeration often used in political rhetoric was conspicuously absent. This influential speech made by the Director of the CIA in 1996 is a case in point:

> My greatest concern is that hackers, terrorist organisations, or other nations might use information warfare techniques as part of a co-ordinated attack designed to seriously disrupt infrastructures such as electric power distribution, air traffic control, or financial

> sectors; international commerce; and deployed military forces in time of peace or war ...

Certainly, the references to the power grid, air traffic control and so forth are in keeping with the sensationalist claims of politicians of a later date, but the language is relatively measured. The issue is couched in terms of 'concern' and 'serious disruption' rather than 'fear' and 'catastrophe'. He continues:

> ... International terrorist groups clearly have the capability to attack the information infrastructure of the US, even if they use relatively simple means. The methods used could range from such traditional terrorist methods as a vehicle-delivered bomb to electronic attack.
>
> The latter methods could rely on paid hackers. The ability to launch an attack, however, is likely to be within the capabilities of a number of terrorist groups, which have increasingly used the Internet and other modern means for their own communications.
>
> Many of the tools and technologies needed to penetrate computer systems and launch information warfare attacks are readily available to foreign adversaries. However, we need to remember that a threat is comprised not only of a capability, but also an intent. *John Deutch, Director of the CIA, from a speech given to the US Senate Governmental Affairs Committee 25 June, reproduced in The Observer, 7 July 1996*

Deutch therefore emphasises that what he is describing is a possibility, rather than a probability, and therein lies the difference between the language of law enforcers and that of politicians. The underlying message here is that terrorists may be capable of cyber-attack, but they may not yet have much of an incentive for it, since conventional methods are still much more certain, accurate and are arguably easier.

After 9/11, the press reports rather more comment by law enforcers on the possibility of cyberterrorism. In the US, law enforcers have tended to put effort into maintaining the profile of cyberterrorism since 9/11 rather more than their UK counterparts.

> Recent reports by the FBI and the Department of Homeland Security have outlined the continuing danger of terrorist groups turning to the internet. One particular concern is that cyberterrorism might be timed to coincide with a physical terrorist attack, such as bombing a building while simultaneously disabling the emergency response system, to ensure that the maximum number of lives were lost. *The Guardian, 24 April 2003*
>
> Keith Lourdeau, FBI deputy assistant director, has told a US Senate committee that terrorists will develop or hire hackers to commit large-scale cyber attacks. *Sunday Express, 30 October 2005*

Yet the general consensus remains that, although terrorists are using information communication technologies for communication, fund-raising and so forth, cyberterrorism is an issue for the future: possible, but not yet likely.

> ... police suspect links between terrorist groups and counterfeiters who use the internet to trade in fake goods. *Daily Telegraph, 19 April 2001*
>
> [Michael Vatis, former Director NIPC] adds: "Terrorist groups are already using technology for sophisticated communications and fund-raising activities. As yet we

> haven't seen computers being used by these groups as weapons to any significant degree, but this will probably happen in the future." *Daily Telegraph, 1 March 2001*
>
> "We have pretty good consensus on what the intention of the terrorists is, but we have no real clue about their capability. US-European co-operation on the intent versus capability debate is absolutely vital," says Roger Cressey, former director of transnational threats at the US National Security Council. *Financial Times, 27 June 2005*

There is widespread concern, however, about terrorist use of the Internet to assist them in conventional methods, such as criminal methods of fundraising, including fraud and counterfeiting, as well as planning and propaganda:

> Terrorist organisations and top criminals are starting to use the Internet to send secret messages and carry out fraud and counterfeiting, according to a new police study. *The Independent, 29 May 1997*
>
> Defence and law enforcement experts are convinced that the attacks on the World Trade Centre and the Pentagon were planned, at least in part, using e-mail and the internet. It is likely that these files would have been encrypted and could only have been decoded by people in possession of a special software key ...
>
> ... Michael Vatis, former head of the FBI's National Infrastructure Protection Centre, said: "It is demonstrably the case that terrorists are increasingly using this technology to thwart lawful government efforts to gain vital intelligence and thereby to prevent terrorist attacks." *Daily Telegraph, 21 September 2001*
>
> US intelligence sources said that websites ... are now central to the efforts of Muslim fundamentalist groups not only bringing in funds but also being used to promote extremist opinions. *Independent on Sunday, 28 October 2001*

There is also concern that information freely available on the Internet, such as security vulnerabilities, might prove useful to terrorists.

> Police officers and security experts have expressed concern. What these people are doing is providing information which could be used by criminals and terrorists," said Bill Hughes, a West Yorkshire assistant chief constable and secretary of the technical and research committee of the Association of Chief Police Officers (Acpo).
>
> Members of the group, however, believe they are highlighting security loopholes which could and should be filled. *Sunday Times, 12 May 1996*

In the UK, pressure on the security services to increase efforts to secure critical information systems seems to come more from government rather than from within, possibly because police and security services still perceive the greatest threats to be from conventional attacks and that prevention of these is, therefore, a better use of their limited resources.

> E-commerce minister Douglas Alexander yesterday ordered internet security to be stepped up. He warned web experts from MI5, the MoD and GCHQ that increased vigilance was needed as terrorists could inflict major economic damage by bankrolling rogue computer hackers and infecting systems with a lethal virus. *The Mirror, 27 September 2001*

The question is, why does the Minister need to warn the security services of the threat from cyberterrorism and order them to act? The security services must be well aware of

the threat and surely take system security very seriously. The Minister felt the need to state publicly that "Something must be done and this Administration is doing it", yet the security services did not feel that such rhetoric was necessary.

3.2 The international effort

Following the publication in 1997 of the report of President Clinton's Commission on Critical Infrastructure Protection, the National Infrastructure Protection Centre (NIPC) was established in 1998 and was the first single, national agency with responsibility for cyber attack. Uniquely, it combined advisory and investigatory functions. The creation of this agency was, itself, the result of a certain amount of lobbying on the part of law enforcers:

> When he came up with the idea for a national organisation that would both investigate cyber crimes and warn the public and private sectors of potential viruses and other assorted forms of digital mischief in 1997, [Michael] Vatis [first Director of the NIPC] says: "There was no genuine system in place to help the government deal with specific cases of cyber crime."
>
> Until recently, computer viruses and online credit card fraud were generally considered to be minor hazards rather than as significant threats to national security.
>
> He says: "My first major challenge was to convince policy makers and the public that internet security was a serious problem that needed to be addressed."
>
> Brandishing the rhetoric of a Judiciary Committee speech, Vatis says: "Cyber crime is not just a law-enforcement problem, nor a defence problem, nor a counter-intelligence problem, nor a business problem. It is all of these." *Daily Telegraph, 1 March 2001*

This rhetoric was influential in the UK, as it was intended to be. The problem, of course, is that cybercrime is a global phenomenon, so the US law enforcement rhetoric on cybercrime and the potential for cyberterrorism was particularly important in persuading other nations to follow suit. Once established, these new computer crime units around the world would be able to share information and work together to apprehend offenders.

> Now other countries such as the UK, Japan and Canada are following the lead of the NIPC and establishing their own cyber crime units, which is a great relief to Vatis given the international nature of internet crime and the difficulties of co-ordinating investigations across borders.
>
> He explains: "If a cyber crime takes place in the States, but the internet address is abroad, we are powerless to do anything.
>
> "Cyber crime is a global issue and we routinely have to work with foreign partners."
>
> The NIPC enjoys a particularly strong relationship with the UK's National Infrastructure Security Co-ordination Centre (NISCC), established in late 1999. When a hacker from Wales known as Curador stole as many as 28,000 credit card numbers from e-commerce websites around the world, the NIPC and NISCC worked with the Welsh police to track down the offender. *Daily Telegraph, 1 March 2001*

> NISCC is working with the FBI in the hunt for the programmer, or group, which planted the love bug virus. Victims included Microsoft, Ford, the CIA and the Pentagon in America, and Vodafone AirTouch and Parliament in Britain. *Sunday Times, 7 May 2000*
>
> [Chief Superintendent Len Hynds] says: "The aim of year one is to get the [NHTCU] up and running and to scope out the extent of the problem. We have no operational goals, although we are heading some investigations."
>
> Four investigations, to be precise, with European and American involvement, although he refuses to disclose any further details. *Daily Telegraph, 19 July 2001*

Clearly, these developments benefit all parties, not just US law enforcement. Yet US involvement does not appear to stop at urging the creation of new national agencies capable of cooperating internationally on cybercrime. They also appear to be involved in European efforts at creating a pan-European cybercrime unit:

> The Bureau also has a shadowy position on European Union committees, tussling with the task of developing a single cross-border cyber crime unit. *The Guardian, 1 August 2002*

The new spirit of international cooperation was used to the full in the weeks and months following 9/11. The international links between law enforcement agencies were relied upon in tracing the activities of the suspects:

> Millions of pounds secretly controlled by the terrorist leader or associates are thought to be washing around the Western banking system. The CIA is understood to have a team of computer hackers siphoning money away from suspect accounts.
>
> British investigators believe they may have uncovered a channel of bin Laden funds from Saudi Arabia to London. US sources say money was transferred from Riyadh bank accounts to a Saudi-owned financial institution in the City, now being investigated by the British authorities. *The Observer, 16 September 2001*

There was also an impetus towards transnational legislation, rendering legal barriers to counter-terrorism as low as possible and giving law enforcement agencies greater powers:

> The European Commission is rushing through a new set of anti-terrorist proposals to create a single EU system, ending the "cacophony" of 15 separate sets of laws and policies.
>
> The new law, to be announced tomorrow, will broaden the definition of a "terrorist", greatly expanding the powers of law enforcement agencies. It will cover anyone accused of aiding and abetting acts of terror rather than confining it to members of proscribed organisations. *Daily Telegraph, 18 September 2001*

This progress has not halted in the years since 9/11, and international cooperation has been strengthened further to the benefit of police officers investigating trans-national crime.

> Chief Superintendent Mick Deats, who heads the 57-strong NHTCU, said: "The internet has no geographical boundaries. It is completely porous, and is therefore seen as a low-risk arena as an attack can be launched from any remote region of the world."

> The unit has recently been helped by new cross-border agreements. *The Guardian, 13 November 2004*
>
> [There has been] a United Nations conference aimed at increasing international co-operation among law enforcement agencies to combat a range of threats from terrorism to corruption, drug trafficking and cybercrime. *Financial Times, 23 April 2005*
>
> The US investigation was carried out with the aid of the UK's national hi-tech crime unit. *The Guardian, 9 June 2005*
>
> He was tracked down and arrested in November 2002 by officers from Britain's National High-Tech Crime Unit after an urgent appeal for help from security officials at Nasa. *Independent on Sunday, 12 June 2005*

Nevertheless, there are emerging problems with this new, necessarily international, approach. Where law enforcers from different countries are forced to work together, the inevitable differences in ethos will occasionally give rise to friction and missed opportunities.

> The transatlantic differences have been starkly revealed.
>
> Last August the UK police were forced to launch a series of arrests when the US authorities announced that a terrorist cell had carried out surveillance of buildings in New York and Washington. The publicity incensed the UK police, who were forced to arrest several suspects before substantial evidence had been gathered against them. In a second incident the US refused to provide evidence to a German court, which led to the collapse of a terrorist trial this year.
>
> Greater transatlantic co-operation between police and judicial authorities is now seen by counter-terrorism experts as essential to both streamlining operations and producing more accurate and specific threat assessments. *Financial Times, 27 June 2005*

Summary

Law enforcers are most concerned with cybercrime and use of the Internet by criminals and terrorists, especially for communication. They rarely resort to sensationalist rhetoric, however, and the expression of the concerns of law enforcers are characterised by accuracy when describing incidents. Use of the future threat scenario is limited and sensationalist language generally avoided. Law enforcers still consider that conventional crime and terrorism constitute more serious threats than cyberterrorism.

The broad concerns of law enforcers relate to inadequacy of the law to deal with emerging forms of deviance and insufficiency of skills and resources amongst law enforcers to meet the new challenges brought by the Internet. The Internet reduces or removes the importance of geographical boundaries, time, identity and personal resources for the user, but correspondingly increases the importance of these things to law enforcers, since they become significant barriers to intelligence gathering and investigation. Terrorist use of the Internet is, however, a double-edged sword, making terrorist activities, such as recruiting and fund-raising, more transparent than before so long as law enforcers have sufficient access to communications data.

Before 9/11, reported concerns of law enforcers were mostly restricted to terrorist use of the Internet to facilitate conventional forms of deviance rather than cyber-attack. Most future threat discussion came from the US at this time. Post-9/11, however, law enforcers are quoted more on the subject of cyberterrorism, yet they remain more concerned about terrorist use of the Internet to facilitate conventional attacks than about cyberterrorism.

The US was a pioneer in the creation of a single, national agency with responsibility for cyber attack. Nevertheless, US observers saw cyberterrorism as a global phenomenon, and they required assistance from similar organisations in other countries. The challenge was to get other countries to set up these organisations and then to promote information sharing and common intelligence and investigations policies. There is mounting evidence that this process is well underway, with the US and the UK having cooperated on a number of major investigations already.

4. THE INFORMATION SECURITY INDUSTRY

Members of the information security industry may be considered authorities on the risks from cyberterrorism. Information systems risk analysis is an integral part of their business, establishing where the threats lie and whether there are any corresponding vulnerabilities: in this case, is cyberterrorism a threat and how might society be vulnerable? Of course, a large part of this industry's revenue derives from the sale of security solutions. Therefore, insofar as the information security industry can be identified with Cohen's category of 'experts' in the context of a moral panic, it must be admitted that they may have a clear commercial incentive to transmit their concerns about the risks from cyberterrorism. These experts cannot claim to be impartial observers. Nevertheless, commercial imperatives do not inevitably lead to exploitation in the sense of scaremongering for commercial gain.

Given that the concept of cyberterrorism has its roots in computer technology and information security, one might expect that claims made by the information security industry would be reflected in the press coverage of this issue from the time it was first reported in the late 1980s. This has not been the case. Figure 13 demonstrates that press reporting of claims made by the information security industry remained at a low level until after 9/11, at which point the figures rise sharply.

Figure 13 **Number of quotes from information security industry by year**

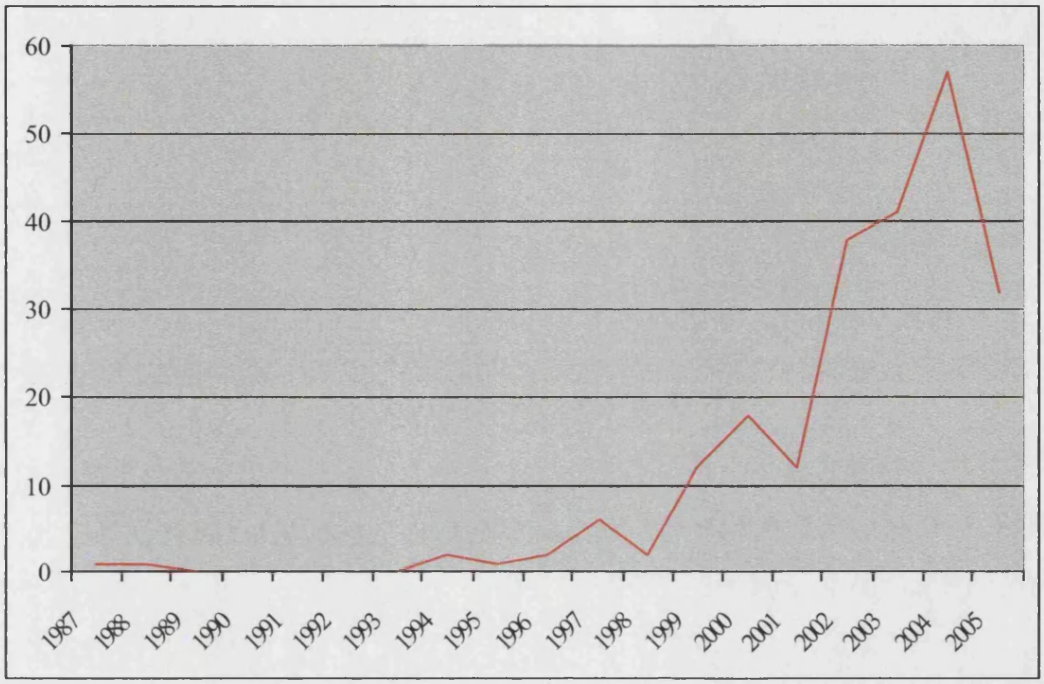


Figure 9 shows that the primary concern of the information security industry is cybercrime. Industry members are almost twice as likely as law enforcers, for example, to express their concern with cybercrime, yet other types of behaviour represented in the taxonomy are of relatively little concern to them. This is most likely explained by the nature of their business: they sell tools to safeguard information and conventional crime, for example, would only ever be of incidental importance. It is therefore unsurprising that the predominant themes found in claims made by the industry and reported in the press are 'hackers' and the 'terrorist link' (Figure 10).

According to Figure 12, industry members are most likely to use the future threat scenario to convey their concerns.

> "I've no doubt hackers will have infiltrated this system already. It's only a matter of time before terrorists do." *Sunday Mirror, 18 August 2002*

They are also likely to exaggerate or distort facts:

> ... someone could hack into an airline system to change the weight allowance on an airliner's payload, causing the plane to crash on take-off or landing. *The Guardian, 5 December 2002*

Nevertheless, they are more likely to attempt to dampen concern than dramatise a situation (Figure 12). The main industry discourse presented in the press centres around the question whether or not concern about cyberterrorism is merited. In the context of press articles dealing with both hacking and terrorism, the overall concern of the

information security industry remains with hacking. When 63 claims in the corpus about specific threats were analysed, 33 relate to hackers and 20 to terrorists. Nevertheless, there is a divide in the industry between those who claim that cyberterrorism is a real threat, with some claiming that it is already with us, and those who assert that this amounts to scaremongering and that there are many real and growing threats other than cyberterrorism which demand attention and resources. As the Guardian points out:

> ...the computer security industry is sharply divided over the seriousness of the cyber-terrorism threat, and there are dissenting voices. Just as with nuclear, biological or chemical weapons, critics ask for the evidence that terrorists have the digital weapons to launch a cyber-attack. *The Guardian, 20 February 2003*

In information security terms, a risk exists where there is a vulnerability in a system, together with the threat of a mechanism capable of exploiting it. There are many established sources of threat to information systems, including hackers and insiders. What has not been established is whether cyberterrorists should be added to this list of sources. Donald Rumsfeld famously outlined three major categories of risk:

> When Donald Rumsfeld spoke of "known knowns", "known unknowns" and "unknown unknowns" the world laughed. But the concepts he outlined are familiar to risk managers.
>
> Computer security knowns and unknowns correspond to risks within systems. A risk exists when a system has a vulnerability and a mechanism exists to exploit it.
>
> Vulnerabilities that can be exploited are quantifiable risks (known knowns), while for those for which there is no exploitation (known unknowns) the impact is unquantifiable.
>
> Security incidents within companies can seriously impact customer confidence and market valuation. Risks can be controlled by ensuring that vulnerabilities are fixed according to their potential impact.
>
> It is clear that the ability of a company to control its risks effectively is inherently linked to its knowledge of exposed vulnerabilities and exploits and the existence of patches for them.
>
> "Unknown unknowns" remain uncontrollable, unquantifiable risks. *Financial Times 21, September 2005*

So, there are established vulnerabilities and there may be established exploits which threaten them. But do cyberterrorists exist? Are they capable of using or creating these exploits? Even if they are, would the results amount to 'terrorism'. Thus the argument in relation to cyberterrorism: is the risk a "known known", such that cyberterrorists do exist and are capable of exploiting known vulnerabilities with catastrophic consequences? Is the risk a "known unknown", such that known vulnerabilities exist, but not whether cyberterrorists are capable of exploiting them with catastrophic effect? Or is the risk an "unknown unknown", where it is known neither whether there exist

vulnerabilities which, if exploited, would lead to catastrophic consequences, nor whether there are cyberterrorists ready and able to exploit them.

The next two sections set out the views of those on either side of this debate.

4.1 Cyberterrorism as threat

In common with other claims-makers in the late 1990s, notably politicians (section 2.2 above), the information security industry voiced concerns that cyberterrorism was a logical next step for terrorist groups, and that the targets would be the economy and the CNI. This was an emerging idea, the public discourse about which was largely triggered by President Clinton's Commission on Critical Infrastructure Protection which published its findings in 1997 (see further section 2.2 above).

> Dr Neil Barrett, an expert on computer hacking and "information warfare" ... predicted that organisations such as the IRA and Animal Liberation Front would soon take advantage of the technology. "It's such an obvious and logical next step, it's something we anticipate," he said. He added that terrorists of the future might use computer viruses to cripple emergency and public services rather than bombs. *The Independent, 29 May 1997*

> Neil Barrett, senior consultant with Bull Information Systems, said terrorists found the Internet an obvious choice for their activities.
>
> "Certainly it is very attractive to them," he said. "Border controls can pick up things like Semtex but they cannot detect computer viruses." Terrorist groups could cause economic damage without the risks they ran in planting bombs. *The Guardian, 29 May 1997*

An obvious next step for terrorists, perhaps, but one which did not materialise in the years that followed. Still, the warnings did not stop and, indeed, gathered force over the years so that the response to claims about the future threat of cyberterrorism grew stronger in proportion to the strengthening conviction of its imminence.

> ...government and private computer experts will be ... look[ing] into the growing possibility of a "cyber-terrorist" attack on what is known as our "critical information infrastructure" – the electronic systems vital for government, armed forces, business, finance, telecommunications, utilities, or emergency services.
>
> There have been warnings from parts of the IT community that terrorists could attempt something like this for at least 10 years, but now governments are taking it much more seriously. *The Guardian, 20 February 2003*

Having predicted a future threat which did not come about, some members of the industry resorted to labelling ordinary criminal and delinquent behaviour 'cyberterrorism'. Thus, the teenager known as 'Mafiaboy', who brought several high-profile websites to their knees, including CNN, Yahoo!, eBay, Amazon and Etrade, became a cyberterrorist. According to the experts, he and his ilk were dangerous and here to stay.

> ... Rick Broadhead, an internet consultant, said cyber attacks would continue. 'We shouldn't feel any more safe because of this arrest,' he said. 'It is a new form of terrorism called cyber-terrorism. I really believe it won't go away.' *The Guardian, 20 April 2000*

In a similar vein, there have been claims from the information security industry that certain high-profile viruses have originated with terrorists. In response to the widespread disruption caused by the 'I Love You' virus (aka 'Love Bug'), for example:

> Experts warned that the attack could have been an attempt by "cyber terrorists" to hack into sensitive systems. One said: "The worrying aspect is that cyber terrorism has become relatively easy and we haven't seen the last of it." *The Express, 5 May 2000*

In addition, the discovery of a variety of security faws became grist to the mill for claims that terrorists were at work.

> Private security companies also say there is growing evidence of attempts at electronic terrorism. "They are trying to get in through the back doors of office networks, which are quite vulnerable," said Christophe Huygens of Belgium-based Ubizen. *The Guardian, 12 August 2002*

As with the Love Bug, this was another case of hacking activity being labelled 'terrorist'. There has also been a tendency for security professionals to pick up on the latest security flaw and claim that it could be used by terrorists, making use of the future threat scenario. When a security flaw was discovered in Downing Street, security experts feared that it:

> ... could be used by terrorists to wage electronic warfare on the Government as the world braces itself for the first anniversary of the September 11 attacks on the World Trade Center. *Sunday Mirror, 18 August 2002*

More recently, in response to a series of security flaws found in Microsoft's Internet Explorer a security professional claimed that:

> ...banks and governments are at risk from organised crime and terrorists. All the hackers need to break into any computer system running Microsoft's Internet Explorer is for a single user at an organisation to log on to the internet on Monday morning using Explorer. *The Business, 13 June 2004*

To recap the findings of this section, when claims that cyberterrorism is inevitable remained unfulfilled many years later, some members of the information security industry either relabelled criminal behaviour 'terrorist' or claimed that certain security flaws could be exploited by terrorists. In this way, the connection between terrorists and cyber-attack has been maintained. One company, however, has done more to perpetuate this state of affairs than any other. 7% of *all* information security industry claims (both for and against cyberterrorism) in this corpus can be traced to Mi2g, an information security company whose Executive Chairman, DK Matai, is widely quoted

in the press. Of the claims which specifically relate to cyberterrorism (n=56) 25% (n=14) originate with Mi2g.

The first quote from DK Matai to appear in the press on the issue of cyberterrorism occurs in 1999, a time when levels of press reporting of information security industry opinion are still very low (Figure 13).

> DK Matai, managing director of Mi2g, said: "The internet attacks from pro-Serbian elements highlights, for the first time, political activism as a force for cyber terrorism.
>
> "You can have a small bunch of people in relatively feeble countries which have been attacked by the mightiest forces in the world. And they have responded effectively via the internet, which allows them to exercise muscle without having the firepower." *Sunday Times, 15 August 1999*

Matai was referring to emails containing pro-Serbian propaganda and website hacks perpetrated by Serbian sympathisers during the war in the Balkans which hit the websites of companies in Nato countries, notably the US and UK. The term 'political activism' might fit, but no terrorist element was established. Even if the attacks had been perpetrated by hackers connected to paramilitary groups (a claim made by Mi2g), the damage amounted to little more than vandalism and certainly does not fit any common sense definition of terrorism.

Recently, Mi2g have concentrated on what they see as the threat from pro-Islamic groups and have noted a rise in ideologically-motivated hacking activity.

> There is now evidence that the cyber-terrorist net is widening to include a larger number of firms...
>
> "This indicates terrorist groups are targeting smaller companies than before and are also focusing on attacking ISPs (internet service providers), where a single penetration can take down 500 corporate websites," an Mi2G spokesman said. *The Business, 3 November 2002*
>
> But now ideologically motivated hacking is rising fast, says ... Mi2g. Its study of major hacker groups active in 2002 notes: "Attacks on the west show a spurt of growth mainly coming from radical groups and individuals based in predominantly Islamic countries." ... "The true extent of the shared agenda between hacktivism and terrorism is only now becoming visible," says the report. "There is a requirement for government-funded network monitoring to go deeper into ideological hacking and to establish the common connections between digital attacks and physical terrorism." *The Guardian, 20 February 2003*

Matai and his company present the hacking activity logged by Mi2g's researchers as being underpinned by Islamic terrorist groups. It is impossible to ascertain whether they are correct in their presentation It is, however, possible to say that they are quick to label this hacking activity 'cyberterrorism' in circumstances where they provide no solid evidence of terrorist involvement other than the finding that some attacks apparently have their source in "predominantly Islamic countries". Matai is also quick

to claim that the CNI is at risk from these sources of attack and, in one of the excerpts below, claims that pro-Islamic groups are working on such attacks even now.

> ... Matai says data attacks are more of a nuisance than a terror but "command and control" attacks on water, power, transport, telecommunications or aviation hubs could be fatal. Once inside the control systems, hackers may choose to turn off power or water supplies, open dams or empty sewage into rivers. *The Guardian, 20 February 2003*

> DK Matai ... said: "There is evidence linking the increase in computer attacks to British support for the US policy on Iraq.
>
> "In fact, even prior to last summer the proportion of attacks by cyber terrorists from pro-Islamic sources was negligible. Now we estimate that at least 15 per cent of digital attacks are from these sources. A range of pro-Islamic groups are working together to target the infrastructures of countries such as the UK and the US." *The Times, 24 February 2003*

In common with other industry sources, Matai has also used damage from high-profile viruses to argue that attacks on the CNI may be imminent. On the Mydoom virus:

> DK Matai ... said the 'frenzy of destruction' had not slowed down at the weekend as much as hoped.
>
> 'There could be more attacks in the near future that could push the boot further than Mydoom and cripple airline services, telecommunications and other critical infrastructure,' he added. *Daily Mail, 3 February 2004*

In fact, Matai and Mi2g are not making claims which are radically different from some other members of the information security industry. However, it is worthy of note that a company wishing to acquire a high media profile is able to do so with an aggressive promotion strategy focussing on newsworthy issues, making their claims more likely to be reported by the press and heard by the public.

Having considered the positive claims made by members of the information security industry about cyberterrorism, the following section will set out the claims of those who claim that the issue is a distraction from more pressing risks.

4.2 Cyberterrorism as distraction

There is a significant body of opinion in the information security industry which holds that scaremongering and wild claims may bring the industry into disrepute, and this may account for why the industry is more than twice as likely as other claims-makers to dampen concerns about cyberterrorism (Figure 12). As Mike Barwise, consultant at Computer Security Awareness, says, one problem with scaremongering is that:

> There's a risk of fulfilling the terrorist purpose ourselves. If we spread the terror ourselves they can sit back and relax. *The Guardian, 20 February 2003*

There are other problems with labelling as 'cyberterrorism' acts which do not actually originate with terrorist groups. A particularly problematic virus, for example, may

cause widespread damage and be genuinely worthy of a sustained attempt by law enforcers to track down the perpetrator and bring him to justice. However, if investigators focus on the idea of cyberterrorism, this may lead to erroneous lines of investigation and use of the wrong type of police resources.

> Many experts also say the security agencies are looking in the wrong place. Mike Bluestone, director of Berkeley Security Bureau, said those who launch virus attacks are more likely to be 'cyber-vandals' not 'cyber-terrorists'. 'Terrorists make targeted demands and like a high degree of control over their operations. A supervirus is more likely to be the brainchild of a spotty adolescent than some terrorist mastermind.' *The Observer, 7 May 2000*

Similarly, politically-motivated hacking, such as the attacks on NATO's website in the course of the Balkans War and the reciprocal website defacements perpetrated by Palestinian and Israeli hackers, is disruptive and often embarrassing, but it is not terrorism and a solution to the problem does not require the Draconian measures appropriate to terrorist acts. All that is required is decent web security, yet the perception that the problem is more serious stands in the way of this. Winn Schwartau, a leading information security professional, argues:

> You have some perception problems with the media. For example, the Nato site (www.nato.int) was attacked but that's meaningless – as is the Palestinians and the Israelis defacing each other's sites (http:/nmit.georgetown.edu/papers/wtaggert.htm). What astounds me is that solving that problem technically is child's play yet none of them are bothering to do it. It's basically just graffiti. *The Guardian, 20 February 2003*

What, then, do the industry members on this side of the fence present as the true position with respect to cyberterrorism? It should be emphasised here that there is no particular reason why the information security industry should be any more aware than other civilians of the occurrence of terrorist incidents, given that information about terrorist attacks may be classified and available only to certain sections of government and the security services. One popular argument is that conventional terrorist attacks are much more certain to hit their mark and much more effective means to generate terror. Cyberterrorism, on the other hand, whilst theoretically possible, is much more difficult to achieve and is more likely to cause disruption and annoyance rather than fear. A senior security analyst for BindView Corporation argues:

> "Cyberterrorism is a catchy phrase and seems to be a hot topic. I'm not saying that a hack could never lead to someone's death, but it's much easier for a terrorist to throw a knapsack of poison into a reservoir than to do something remotely with a computer ... If I knew George Bush was going into hospital and would be on a life support system, conceivably I could interrupt the power grid or hit the back-up batteries in the middle of his operation. But most of these systems already have a lot of safeguards, mainly just to prevent simple accidents." ...

> ... "From a global perspective, I am far less concerned about cyberterrorism and hacking than acts of terrorism in the physical world. With bombs going off around the world and everyone wondering when al-Qaida will strike next, who cares if a web server gets hacked?"
>
> He admits he would be as annoyed as anyone if his web site was hacked or defaced: "But you couldn't justify diverting large amounts of resources from anti-terrorism in the physical world to protect my assets in the virtual world." ...
>
> ... some of these cases are legitimate causes for concern, but ... usually, cyberterrorism is a sideline affair. "It's a lot easier to blow up a pipeline in the middle of nowhere than it is to hack your way in over a computer terminal ... A single car bomb in the right place in Wall Street, in conjunction with the events of 9/11, would have taken out the US financial system. Not a hack."
>
> Such "force multipliers" can make a terrorist attack a great deal worse. "Using hackers in conjunction with real world events would have more impact, but just bringing down a web server does not." *The Guardian, 5 December 2002*

So, the argument goes, a pure cyberterrorist attack is unlikely for the most practical of reasons: a conventional attack is much easier to achieve. Other industry members hold that claims about cyberterrorism should be backed by evidence, and the available evidence shows that a serious attack by terrorists is unlikely, first, because few hackers exist with the skills to accomplish a targeted attack and, second, because the inside information they would need is extremely hard to access.

> "Before we make assertions we must justify them with evidence," says Barwise [consultant at Computer Security Awareness], and he reckons we don't yet have a lot of evidence that terrorists either do or don't have the skills. Most attacks are by "graffiti writers" on websites, he says, and then come the less common hacks into systems for financial fraud or other personal gain. Rarest of all are what he calls the "uber-hackers": the one or two per hundreds of thousands of hackers who are good enough to hack into government systems and yet cover their tracks. "That isn't prevalent," he says, "and it's difficult to see how serious damage could be caused by someone not equipped with insider knowledge – they've got to know about the technical aspects of the system they're trying to damage."
>
> This is why Peter Sommer, of the London School of Economics Computer Security Research Centre, dismisses the idea of an impending "electronic Pearl Harbor". The number of people in government who know the sort of sensitive security information that terrorists would need is very few, he says. *The Guardian, 20 February 2003*

Some experts have emphasised that terrorist cyber-attacks on the CNI would be extremely difficult to achieve since they are usually isolated from the Internet. In any event, there will usually be contingency plans for service problems which already happen by accident, human or otherwise. The easier types of cyber-attack, such as attacking web servers, are merely disruptive and not particularly eye-catching from a terrorist's point of view.

> Counterpane's Schneier contends that these kinds of attacks are harder to execute than simply hacking a server, since most of the computers critical to running power plants and air-traffic control systems are usually not connected to the internet. Disrupting the internet with worms or denial-of-service attacks is not particularly attractive to terrorist

> groups since they lack the impact of a bombing or hijacking. "Not being able to access the internet does not induce terror or fear in people. Terrorists are out to cause fear, not inconvenience," he says.
>
> And even should a cyberterrorist attack prevail and shut down the power grid or disrupt the emergency response system, "These sorts of outages and problems tend to happen by accident already, so we have workarounds for them", Schneier argues. "What we don't have workarounds for are people flying planes into buildings or blowing up embassies." *The Guardian, 24 April 2003*

Schneier repeated this assertion a couple of years later, adding that he thought the spectre of cyberterrorism was largely a media creation.

> ... Bruce Schneier, a leading cryptographer and founder of Counterpane Internet Security, points out that such attacks are yet to happen. The threat is somewhat overlooked because it is also overblown, he suggests.
>
> "I think it's largely a media creation. We know what terrorism is - it's planes flying into buildings, it's not that you can't get your e-mail," he says.
>
> "Even something as serious as major outages that have been accidents - there's a reasonable argument that the 2003 North-East (US power grid) blackout was the result of a computer problem, but even if al-Qaeda were to do it, they would not call it terrorism – it's bad, it's expensive but no one would be terrorised." *Financial Times, 16 November 2005*

Some industry research confirms this view, finding that there has been no cyberterrorist attack on the CNI.

> Despite fears that terrorists would use the internet to cripple infrastructure such as power grids, financial systems and telecommunications networks, the research [conducted by Symantec, a provider of internet security services] showed that there had not been a single case of cyber terrorism in the six months to December 31. *The Times, 3 February 2003*

The arguments above should not lead us to suppose that there is nothing to worry about. On the contrary, proponents of this view are concerned that, in focussing on the issue of cyberterrorism, society ignores the very real problems of cybercrime to its cost.

> Iain Franklin, the vice president of Entercept Security Technologies Europe, claims that hackers are currently gaining the upper hand, and points to the sharp increase in the number of website defacements reported over the past six to nine months. He believes the implications for e-commerce sites are extremely serious as an attack could lead to a loss of online consumer confidence. But while he agrees that it is theoretically possible that vital supplies such as water and power could be affected by hacking, he believes it is unlikely because hackers tend not to work in a coordinated way. *The Guardian, 19 April 2001*
>
> Some security experts wonder whether it makes sense to emphasise cyberterrorism when there is a more immediate danger from cybercrime and other online maliciousness. The SQL Slammer worm, which struck computers earlier this year, causing considerable damage, is not believed to be the work of either terrorists or a hostile government. "Our networks really are insecure, and there is lots and lots of crime: that is our biggest problem," says Bruce Schneier, founder and chief technical officer of Counterpane Internet Security. His hope is that companies strengthening their security in response to the perceived risk of cyber terrorism will have the net effect of

> reducing what he sees as the real danger – the rising level of criminal activity online. *The Guardian, 24 April 2003*
>
> "There is a general danger of cyber-terrorism but there are more immediate and direct threats to the infrastructure, and if you have limited money, I would chase the other threats before cyber-terrorism," ... many of the strategies that corporations are adopting to protect themselves against ordinary hacker attacks will also serve them well if terrorist organisations such as al-Qaeda strike. *Financial Times, 16 November 2005*

This brings us to the point at which most industry insiders meet, regardless of their perspective on the cyberterrorism argument. Whether an organisation or individual is trying to protect itself from cyberterrorism or from cybercrime, the security solutions are very similar, if not identical.

Summary

Members of the information security industry may be experts in the sense that they are socially accredited as such to "pronounce their diagnoses and solutions" (Cohen 1972), but they have a clear commercial incentive to convey concerns about cyberterrorism. However, the industry is split between those who promote concerns about cyberterrorism and those who consider it scaremongering, there being other, more pressing problems worthy of resources. Although the future threat scenario, exaggeration and distortion are the favoured mechanisms by which concern about cyberterrorism is conveyed, a significant section of the information security industry is also quite likely to dampen concerns. Overall, the industry remains predominantly concerned with cyber-criminality, rather than cyberterrorism.

The press started to report the concerns of those in the industry who consider cyberterrorism a significant future threat in the late 1990s. The warnings did not stop when the threat did not materialise, however, and warnings gathered force regardless. Various mechanisms have preserved the perception of the immediacy of the threat: labelling cybercrime 'cyberterrorism'; claiming high-profile viruses have originated with terrorists; claiming certain security flaws will be exploited by terrorists. One company, Mi2g, accounts for a disproportionate number of industry claims on cyberterrorism reported in the press. This demonstrates that those who are prepared to market themselves aggressively will get their claims reported and, therefore, heard.

One the other side of the industry there are those who argue that those broadcasting the threat from cyberterrorism risk fulfilling the terrorist purpose themselves through scaremongering. Mislabelling crime as terrorism may lead to erroneous lines of investigation, misuse of resources, or inaction through fear. Proponents of this view argue that conventional terrorism and conventional cybercrime are much more serious

threats and society's resources should be directed there. Although cyberterrorism is theoretically possible, it is difficult to achieve without insider knowledge and unlikely to cause the brand of breathtaking violence which is most likely to inspire fear. It is argued that there is no evidence of any cyberterrorist attack. Few hackers have the necessary skills and the inside information often needed for success is extremely hard to access. The isolation of the CNI from the Internet and the contingency plans which exist for accidental service problems make cyber-attack even more difficult. Nevertheless, the industry largely agrees that the technical and procedural security solutions are the same whether protection is sought against cybercrime or cyberterrorism.

5. THE RÔLE OF EXPERTS

"... socially accredited experts pronounce their diagnoses and solutions" (Cohen 1972)

When the corpus was coded, it was found that those who might be considered socially accredited experts in the sense meant by Cohen split into two camps: those in the mainstream information security industry and others. Experts from the information security industry are by far the most numerous and most quoted in the press (Section 4). They were coded with the term 'infosec industry'. The 'others' include those in related industries and professions, academics and those referred to by the press as 'experts' but who are never actually identified. It is these others who make up the category of 'experts' in this study's coding system.

Figure 9 demonstrates that experts are most often used in the press to comment on cybercrime, even though these comments may be couched in terms of terrorist activity. Remember that the categories of behaviour in Figure 9 relate to an objective assessment of the behaviour being described and do not reflect the terms in which that behaviour is couched in the article. Figure 10 underlines this by showing that the theme most often used by experts is that of the terrorist link, although the theme of hackers is also an important one for experts. Experts are also more likely to discuss true cyberterrorism than either law enforcers or the information security industry (Figure 9), although the precise source for these quotes is often not identifiable from the article and the language used is often of the type "Experts say that...".

The rhetorical mechanisms most often used by experts for presenting their arguments are exaggeration/distortion, the future threat scenario and dramatisation (Figure 12). This is consistent with the presentation of mostly sensationalist content relating to the

perceived problem. There is actually relatively little said by experts (other than the information security industry) on what the solutions to cyberterrorism might be.

> When journalists ring you up with their rumour of a hack, their report of evidence of eavesdropping by VDU radiation, their 'steer' from the authorities of a computer fraud about to be frustrated, their anxiety that every other journalist in town is writing about computer viruses, or about subversive or pornographic bulletin boards, what they really want is a validating quote for a slightly rickety story. They can only use your views if they are sensational. Tell the newshounds what you honestly think, and either the story dies or they rush back to the contacts list until they find a more quotable expert. Either way, no publicity for Hugo.
>
> The generally accepted statistic for the incidence of computer crime in the UK is around Pounds 400 million per year. Its authority derives from being frequently quoted. A rich publicity reward awaits the 'expert' who announces that this is a huge underestimate. A much less attractive prize is in store for the sceptic who says, on the contrary, there is hardly any computer crime at all. *The Guardian, 5 May 1988*

This piece by Peter Sommer, writing as Hugo Cornwall, author of *The Hacker's Handbook*, underscores nicely the dialectic between, on the one hand, the press and the filtering process which is central to the search for a newsworthy story and, on the other hand, the 'expert', who so very often has a vested interest in being quoted, whatever it is that he chooses to say. Experts are most often sought out by the press to give weight to a story which has a sensationalist angle to it. There may also be times when an individual or organisation goes to the press with sensationalist claims as a profile-raising exercise. The claims made by Mi2g, detailed in section 4.1 above, are an important example of this. However, there is also a relatively strong representation amongst experts of the view that cyberterrorism has been blown out of all proportion, and this shows up as panic dampening activity in Figure 12, an activity which is significant amongst experts. As with the information security industry generally, experts display a high degree of heterogeneity in terms of the views expressed. And, of course, views are not static and change over time, as Simon Davies of the LSE points out:

> Looking back to, say, 1996, it seems everyone from the G7 to the man-in-the-street was convinced that the Internet equated to anarchy. Cyberspace, they believed, could never be controlled by any government – totalitarian or otherwise. This is still the common view.
>
> But now, those same civil rights advocates have turned on a sixpence, and are warning that the world is on the brink of an era of unprecedented mass censorship. Far from being a morass of anarchy, it turns out that the Internet is homogeneous and orderly – ideal conditions for control. *The Independent, 4 September 1998*

What, then, can be said about the patterns which emerge from the contributions of experts to the UK national press? Certainly they have plenty to say about cyberterrorism, but it is interesting that the majority of these references are to 'experts'

who are never fully identified: the mention of the word 'expert' is meant to add weight to a statement and the reader is expected to take them at face value.

> So-called 'secure' information systems are vulnerable to attack from terrorists and hostile regimes, say the experts. The attacks, they contend, have already begun: the only reason we haven't heard much about them is because either the victims don't know they have been targeted yet, or they would rather keep it a secret. *The Guardian, 22 May 1997*

This example is archetypal. The reader is not told who these 'experts' are but their citation as the source of this information is meant to add weight to the associated claims. The claims made about the problem are not particularly robust. Secure information systems may be vulnerable to attack from terrorists and hostile regimes, but where is the evidence that they are willing or, indeed, able? The claim that such attacks have already begun but the public has not yet heard about them seems far-fetched without the provision of more evidence or at least an assertion that classified evidence to this effect probably exists. Why, for example, would a terrorist attack in secret or in such a way that the victim does not know he has been attacked? This would preclude the spreading of fear, an essential element in any definition of terrorism. Secrecy is the hallmark of crime, not terrorist attacks. This claim is analogous to the future threat scenario: the former cannot be disproved because it is kept 'secret' or has not yet been discovered; the latter cannot be disproved because, by definition, it has not yet happened.

Of course, unidentified 'experts' are widely used to give weight to bald statements of future threat scenarios:

> The work of these hackers throughout the developed world first alerted international leaders to the dangers. One computer expert said: 'Up to now most of the hacking has been done for fun but if the know-how of these people ever fell into the wrong hands – those of terrorists or political extremists – the consequences could be catastrophic. *Mail on Sunday, 14 February 1993*

Whilst hackers are certainly capable of causing widespread disruption and a reasonable of economic loss, the words 'danger' and 'catastrophic' do seem rather out of place. Such terms seem to be justified by the addition of the terrorist angle, but the 'expert' is making a leap too far. He does not show how a catastrophe might be caused by a terrorist or extremist, or even whether it is possible. Similarly, readers are asked to accept at face value the experts' claim that cyberterrorists are capable of attacking transport and communications systems, with or without the additional justification of the spread of the Mydoom virus:

> Internet security experts say the speed with which Mydoom has spread and the scale of the damage suggests that companies have failed to properly educate employees about the dangers of viruses. They say it shows how vulnerable the world's computer systems are at a time when concerns are mounting that 'cyber terrorists' could use viruses to paralyse transport and communications systems. *Daily Mail, 3 February 2004*
>
> Experts have warned that the world's computer systems are increasingly at risk from 'cyber terrorists' who could paralyse transport and communications systems. *Daily Mail, 4 May 2004*

In this excerpt, 'experts' are used to validate a future threat scenario of disaster caused by cyberterrorism which would be on a par with other, better known, forms of calamity:

> Experts believe cyber terrorism is as strong a threat to the United States as nuclear, chemical or biological proliferation. *The Times, 10 October 1997*

By linking the concepts of cyberterrorism and nuclear, chemical and biological disaster in the same sentence, it is implied that a cyber-attack would be every bit as nightmarish as one of the latter scenarios. Specifics of how the attacks would be executed are not discussed in this article, but the next example goes a stage further by citing experts' claims that terrorists may use the Internet to cause chaos, train collisions and attack the CNI:

> Experts say there is growing concern that terrorist groups are trying to use the internet both to communicate and to launch cyber-attacks on US and British companies and government bodies in order to create chaos. Experts believe the software could allow terrorists to cause train collisions by hacking into rail companies' computer systems. There is also the potential for sabotaging water, gas and electricity supplies in the same way. *Sunday Times, 14 October 2001*

'Experts' have also been used to back claims that terrorists, including al-Qaeda, are behind hacks on Whitehall systems.

> Terrorists are feared to be behind an alarming rise in hackers' attacks on top-secret government computer files. Home Office figures obtained by the News of the World show sinister cyber raiders are making an average of 18 attempts a day to break into the key systems. Experts believe that terrorists – including Osama bin Laden's al-Qaeda network might be trying to steal sensitive British and American military information. *The News of the World, 24 March 2002*

Whilst it is well-known that government systems have always been targets for hackers, there is little evidence that any of these hacks have been perpetrated by terrorists and it would be interesting to know which 'experts' were behind this claim.

All of this gives a good flavour of how 'experts', who are never actually identified in the relevant article, are used to give weight to sensationalist portrayals of the dangers from cyberterrorism. This trend is very much media-driven. A journalist decides on an angle he wants to take and then justifies that by reference to a nameless 'expert'. However, there are many other issues on which experts have pronounced, indeed too many to list here. Where claims are made about specific issues, the unidentified

'expert' starts to fade into the background and specified academics and industry figures come to the fore. Sometimes their views are sought out by journalists in order to give weight to certain claims made in a story, as with the previous examples with the nameless 'experts'. But often claims originating with experts come to the attention of the press and form the basis of the story. One such example originated with speakers at an academic conference in Australia in the late 1990s who made of their own motion claims which every journalist dreams of: cyberterrorism is imminent and its results potentially catastrophic:

> International terrorists can now inflict as much damage using computers and information technology as they could with bombs and explosives, according to security experts in Australia. Delegates at the Australian Institute of Criminology conference in Canberra heard that terrorists are increasingly able to use "information warfare" instead of traditional weapons to inflict damage on their targets. They could, for example, hijack air traffic control systems to crash aircraft and cut power lines, or take hostage computerised services such as telecommunications and power supplies. Terrorists were also increasingly able to use the Internet as a tool of destruction, for example by carrying out "e-mail bombings" to throw computer equipment into chaos. Russell Smith and Peter Grabosky, both security researchers, said computer systems everywhere could be vulnerable to disruption by terrorists, pranksters and extortionists, and gave a warning that authorities around the world had so far failed to realise the potential for computer terrorism. They said: "Techniques of 'information warfare' may be employed by terrorist organisations with no less effect than the traditional bomb. Some people regard their information systems with a degree of nonchalance. It's the contemporary equivalent of leaving your home with the door unlocked." *The Times, 18 February 1998*

This apocalyptic vision of the future has probably lost its currency in mainstream academic debate over recent years, even if it is a vision very much current in the political debate, as exemplified by this report written for the US Congress:

> Extremists are recruiting Islamist computer hackers – creating a breed of high-tech terrorist who threatens to cripple Britain's economic infrastructure.
>
> Banks, businesses, Government offices and transport systems are in the frontline of a new wave of cyber terrorism that could bring the country to a standstill and drain billions from the economy.
>
> A new report claims that as physical security in the West tightens, terrorists are looking to exploit vulnerable computer networks and forge new alliances with cyber criminals.
>
> The study warns of a wave of cyber attacks and points to the London bombings in July as evidence that homegrown terrorists are already "embedded" in high-tech organisations. *Sunday Express, 30 October 2005*

Various topics associated with cyberterrorism have fallen in and out of the limelight over time. References to experts in the press are a good barometer of this, since their views on very specific topics are either sought out or reproduced according to the journalistic imperative to give an account of the hot topics of the moment. The issue of viruses is one which has come in and out of focus many times over the last two decades,

and their release has often been associated with terrorism. Citing the concerns of experts in this respect has become a mainstay of press coverage:

> For example, Virus Construction Lab (VCL), a program recently discovered in the United States, promises to make virtually anybody into a "computer terrorist". VCL offers a huge range of viruses, from the merely annoying that flash messages on a computer screen to those designed to destroy the information held in a system.
>
> "The programs are fairly primitive and their effects are not too difficult to sort out," says Edward Wilding, the editor of The Virus Bulletin, a monthly newsletter, "but there is considerable worry that they will soon become more sophisticated and a real danger to company computer systems." *The Times, 18 September 1992*

In 2001, the issue of anonymisers and how they might be used by terrorists gained centre stage. This came in the wake of the 9/11 attacks and in the midst the hunt for bin Laden and his associates. It was clear that any technology which had the potential to assist terrorists in covering their tracks would make the headlines and there were plenty of experts available to add their comment.

> Stephen Whitelaw, Iomart's chief entrepreneurial officer, warned that computer software known as "Triangle Boy", which helps users to operate anonymously, is now the "most dangerous tool for terrorist and criminal networks".
>
> He believes that with anonymous, untraceable access to the internet, groups such as militant Islamic fundamentalists could wreak global havoc.
>
> "It is a potentially terrifying tool, which means that terrorists could communicate or access illegal sites without detection," he said. ...
>
> ... Dr Neil Barrett, a computer security adviser to the British government, said: "It is a concern that people may use this the wrong way. This is a sophisticated anonymiser, which means more people will be able to use this for bad reasons."
>
> He said the software had helped computer users in repressive regimes but admitted it could be used to create widespread chaos. "You could cause phenomenal damage by hacking into computers controlling the electricity grid, and theoretically you could cause two trains to collide," he said. *Sunday Times, 14 October 2001*

In 2004, a technique for hacking into mobile phones, called 'bluesnarfing' after the Bluetooth technology involved, dominated the technology headlines. It was reported that criminals and terrorists might use this technique to dangerous effect, and the experts were called on to comment:

> Ian Angell, Professor of Information Systems at the London School of Economics, described the discovery of the flaw as a devastating blow for the phone companies.
>
> "This could really disrupt the whole industry," he said. "The idea that a perfect stranger could spy on you – that represents a technology too far." *The Times, 14 April 2004*

Another perennial favourite is the issue of insiders creating havoc with computer systems, either disgruntled employees seeking revenge or, more recently, the spectre of terrorists infiltrating key organisations.

> 'It is incredibly easy to do a search on the internet for a program that you can then download and use to read emails round your office,' said Dr Magnus Ranstorp, of the Centre for the Study of Terrorism and Political Violence, at St Andrews University.
>
> 'Then you get recruited by a group or business outfit and used to infiltrate an office with fake credentials. Someone starts working as a temp in one department. After a few weeks, he or she could have gone through half the secure documents in the whole building.' *The Observer, 8 December 2002*

Experts do not, however, confine themselves to comments on the dangers from cyberterrorism. There are many who are vocal on the subject of the dangers posed to society by its response to terrorism. One subject which has been current since at least the mid-1990s is the 'surveillance society', brought about by government's overzealous reaction to the problems of cybercrime and cyberterrorism. Early on in this debate there was much controversy about cryptography, for instance. Some experts, such as Dorothy Denning (1996), advocated technologies which would render encrypted data transparent to the authorities. Others, such as Ross Anderson, saw danger in allowing such unprecedented access to personal communications:

> Academic cryptographers are divided. Ross Anderson of Cambridge University tells the programme: "The transactions which make up our daily lives are rapidly becoming electronic. If we're denied the means to protect them, we're not just talking about hackers and electronic crime. We're talking about a surveillance society in which authority will know every detail of our lives. Even Hitler and Stalin couldn't have dreamt of that." *The Independent, 3 September 1995*

Simon Singh, author of *The Code Book* (Singh 1999), neatly encapsulates the balance which must be struck between security and privacy in relation to the use of encryption technologies:

> Such ciphers would guarantee privacy for all personal and business transactions on the internet and, as such, would seem to be a boon to society.
>
> National security agencies and police forces, on the other hand, see super strong encryption as a potential threat.
>
> It would hinder their ability to monitor the activities of criminals, organised crime and terrorist groups, not to mention paedophile rings, many of which already use sophisticated methods to scramble their communications. ...
>
> ...The challenge for governments and scientists is to come up with a way of allowing law-abiding citizens to have their right to privacy while allowing the police to spy on the bad guys. *Daily Mail, 31 August 1999*

Simon Davies of the LSE has been lobbying governments for many years in an attempt to protect privacies which he considers to be menaced by the creation and use of broad coercive powers ostensibly to address quite narrow issues. As an acknowledged expert in this area with very strong opinions, he regularly writes articles which are published in the press. Here he argues, in relation to measures to combat child pornography on the Internet (a goal which he fully supports):

> If governments can succeed in their strike against one form of expression, why not others? Why not, say, hate speech, marijuana promotion or political dissent? After all, the technology that generates and distributes kiddy porn images is the same technology that processes the traffic on political discussion groups ...
>
> ... A new Europe-wide initiative – "Action Plan for Safe Use of the Internet" – will be established this year. Its intention is to conduct the censorship equivalent of a high-tech driftnet fishing expedition over the Internet, blocking access to content deemed to be harmful, unlawful or undesirable. *The Independent, 4 September 1998*

Davies sees this as inimical to the freedoms offered to us by the Internet and argues for a more refined approach to combating crime and terrorism. Similarly, in response to proposals for enhanced access to personal communications for government agencies, for reasons including, but not limited to, counter-terrorism, some experts have spoken out about their fears:

> ... the legislation could lead to distinctly sinister scenarios. "It's shocking," said Dr Ian Brown, director of the Foundation for Information Policy Research, "Just like the government trying to get information to smear Pam Warren, the Paddington rail crash campaigner, you can imagine that happening all over the country – councillors could gather ammunition on their opponents." *Sunday Times, 16 June 2002*

Other experts, such as Paul Taylor, a sociologist at Salford University, have been more specific in their accusations of 'control of the Internet by the back door':

> ... the authorities insist that the measures [access to civilian internet data without warrant] are essential to combat international crime and terrorism. But others worry that they will be used to monitor and discourage legitimate political activity and will ultimately ensure that only "acceptable" voices are heard on the net. Hacktivists fear that politicians, often lacking technical expertise, will be easily swayed by business. *The Guardian, 2 January 2001*
>
> According to some, exaggerating fears over a possible cyber-terrorist attack is part of that attempt to exert control over the internet. Clearly, hacking and viruses targeted at the West are possible, says Hables Gray [professor at the University of Great Falls in Montana]. "But the good news is that Saddam Hussein is an uninspired, if not incompetent, military leader who fought the Iran and Gulf wars as if they were the first world war. It seems unlikely Iraq will even attack the internet." *The Guardian, February 2003*

Fear and risk are key concepts in the debate on cyberterrorism, and the meta-debate about these very concepts and their place in modern society has been brought to public attention through the press by academics such as Frank Furedi, a sociologist at the University of Kent:

> We seem incapable of embracing innovation or new experience without recasting it as a risk.
>
> The fear of risk feeds on itself. And safety has become the fundamental value of the nervous nineties. Hardly a week goes by without some new danger to the individual being reported, and another safety measure proposed....
>
> ... the Internet has been represented as a potential site for major calamities. There has been much press comment about so-called 'cyber-terrorism' and the threat to society's moral well-being from pornography and paedophile rings. ...

> ... So why has this inflated sense of danger come about? Any attempt at an explanation must inevitably be schematic. But one factor at play could be a collective striving to make sense of the uncertainty created by fundamental changes in human relations. The weakening of traditional forms of solidarity – family and class – has been widely commented on. The consequence of this process has been an intense individuation of everyday life, forcing people into situations where little can be taken for granted. ...
>
> ... Commercial factors may also be operating. There can be little doubt that the culture of fear has been seized upon by astute entrepreneurs. Products and services that are linked to risk avoidance are doing well. *The Guardian, 26 July 1997*

Summary

It is clear that unidentified 'experts' are frequently cited by the press to give weight to sensationalist and unsubstantiated claims about the general dangers from cyberterrorism. On the other hand, many identifiable experts have expressed views about various and specific aspects of the cyberterrorism problem. It tends to be the case that, where specific claims are made, these can be traced back to an expert identified in the article. However, the overwhelming conclusion to be drawn from the contribution of experts to the cyberterrorism debate is that there is a wide range of different claims being made and that, of all the claims-makers, the views of experts are the most heterogeneous in nature. Although the very general, sensationalist claims about cyberterrorism are consistent, in all other respects it is very difficult to draw together coherent strands of argument representing the views held by experts, or a significant group of them. This reflects their mostly reactive rôle, that of responding to press enquiries. On the other hand, it may also speak to the fact that there is a lack of consensus amongst experts about the nature of the problem.

The next chapter extends issues of concern and consensus into the realm of hostility: who or what are the targets of hostility; can a consensus be identified; and how do targets of hostility fit into the belief system which is growing up around the issue of cyberterrorism?

CHAPTER 7

FINDINGS: HOSTILITY AND CONSENSUS

Previous chapters have considered concerns about cyberterrorism and the level of consensus which has been achieved between the different claims-makers. If cyberterrorism is the subject of concern, then cyberterrorists are the object of hostility. In moral panic terms, consensus is relevant to the issue of hostility, just as it is relevant to the issue of concern. Over a period of time, sometimes long, sometimes short, a consensus may develop as to which groups are responsible for the perceived threats to society, resulting ultimately in their definition as 'deviants'. Cyberterrorists are an interesting case: many have claimed that they exist, but there is no empirical evidence in the public domain of their existence, nor any publicly documented example of a genuine act of cyberterrorism.

How, then, can this particular phenomenon be characterised? Cyberterrorism unites a trinity of elements: the hacker, the terrorist and technology. The question which underlies the evidence is this: does the cyberterrorist have his own social identity, or have social understandings of hackers, terrorists and technology evolved to embrace the concept, effectively relabelling existing folk devils? The answer will be provided by analysis of the stereotypes presented in the press.

When the corpus was coded, the three most significant codes overall in terms of frequency were: the code for *hackers*[2] (n=828, rank: 1); the *terrorist link* (n=657, rank: 2); and *technology* (n=449, rank: 3), the code employed for references to technology, including the Internet. The data show that each of the three elements – hackers, terrorists and the technology – have been demonised by claims-makers in the press. By understanding the types of hostility displayed to each of these elements, it is possible to understand how the cyberterrorist has been constructed.

[2] A note on formatting: where terms are in italics, this denotes a code or sub-code which has been derived from the corpus of data.

Because the frequencies of the codes just described were so high, a secondary coding process was necessary in order to effect a more nuanced analysis. Quotations coded with the three primary codes – *hackers*, *terrorist link* and *technology* – were subjected to a secondary coding process which produced several sub-codes for each primary code.

It was noted that different views predominated at different times, so the frequencies for these codes and their sub-codes were distributed over six unequal time periods chosen for their historical significance: late 1980s; early 1990s; late 1990s; 2000-10 September 2001; 11 September 2001-2002; and 2003-2005. The late 1980s refers to the period from 1987 (the first identified UK national press article mentioning both hackers and terrorism) to 1989, a time when the very early thinking about the terrorist link with ICTs was emerging. The early 1990s was the period during which PC ownership became widespread and people became acquainted with computers at school, home and work so that they became embedded in social discourse. In the late 1990s, use of the Internet by ordinary people really took off and its potential was widely debated. The next time period chosen was 2000 to 10 September 2001, being the period between two defining episodes: the turn of the Millennium and the 9/11 attacks. The penultimate time period runs from 11 September 2001 to the end of 2002, a time of intense media coverage and speculation covering the immediate aftermath of 9/11. The final period spans 2003 to 2005, bringing us up to the end of the last complete year covered by this corpus of data. This is a period characterised by war and post-9/11 suspicion, particularly with respect to technology and its potential uses by terrorists and criminals on the one hand, and the authorities on the other.

The remainder of this chapter is organised into three sections which will deal in turn with the analysis of the three primary codes – *hacker*, *terrorist link* and *technology*. At the start of each of these sections will be two charts. The first is a bar chart showing the frequencies of the sub-codes for the whole corpus. The bar charts are also colour-coded to show how the sub-codes are distributed over the time periods described above.

The second chart at the start of each section is a line chart giving data for each time period. This chart is based on the same data used in the first chart, but a compensation has been made to take account of the fact that the time periods are not equal. Take for example Figure 15. In the period 2003-5, there were 217 quotations coded with the primary code *hacker* and 91 of those were coded with the sub-code *criminal.* In order to compare like with like across the time periods, the frequency of the sub-code *criminal* for 2003-5 is expressed as a percentage of the total number of *hacker*

quotations for that same period, giving a value of 42%. In other words, during the period 2003-5, 42% of all the references to *hackers* portrayed them as *criminal.* This contrasts with only 14% in the late 1980s. Over the whole corpus, that is 1987 to 2005 (represented by the thick, red line in Figures 15, 18 and 20), 27% of all the references to *hackers* portrayed them as *criminal.* This gives us a reference point from which conclusions may be drawn in a historically situated manner.

In each of sections 1-3, these charts are then followed by an analysis of the quantitative and qualitative results of the coding process. Perceptions of *hackers*, the *terrorist link* and the *technology* will be considered in a historically situated manner, with a discussion of which features have been amplified and which have been attenuated.

1. HACKERS

During the coding process, 828 quotations referring specifically to hackers were identified. All such quotations were coded with the primary code *hacker.* The vast majority of these quotations referred to hackers in the abstract, as an amorphous group.

The aggregate figures represented in Figure 14 demonstrate the overwhelming predominance within the corpus of views of hackers in the abstract as *criminal* or *terrorist*. Remember, these data concern references to hackers which were found in articles in which both hackers and terrorism are mentioned. However, on an objective assessment, only about 1/5 of these articles (149 out of a total of 681) have as their main subject matter any kind of terrorism, cyber- or otherwise. Despite this fact, it is interesting to note that the view of *hacker as terrorist* comes second only to *hacker as criminal* in terms of frequency. When considering the hacker myth in general, Skibell (2002) found that there was a strong and enduring shift from 'hacker as nuisance' to 'hacker as criminal' around the mid-1980s. These results are entirely consistent with his findings, the surprise being that, in a sample deliberately skewed towards the terrorism issue, *hacker as criminal* still comes out on top by a significant margin.

Hacker as criminal is a perception which has increased in importance over the last 20 years. In the late 1980s, 14% of all references to hackers in the corpus viewed them as *criminals*, compared with a peak of 42% in the years 2003-5. On the other hand, the view of *hacker as terrorist* rose during the 1990s to a peak of 24% and then roughly stabilised. With just under a quarter of all references to hackers labelling them *terrorist*, this is still a very significant theme.

Figure 14 **Cumulative frequency distribution of *hacker* sub-codes by time**

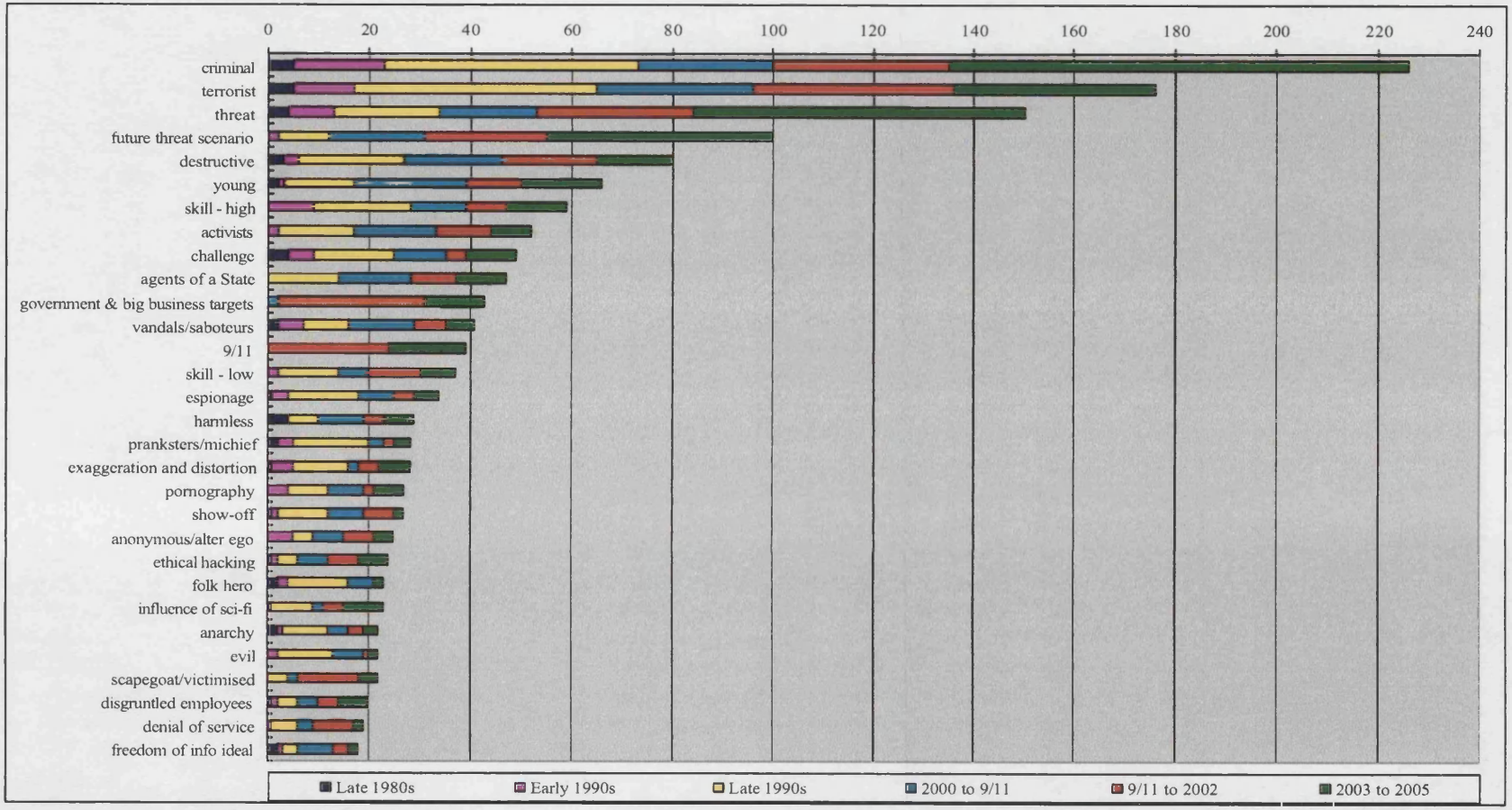
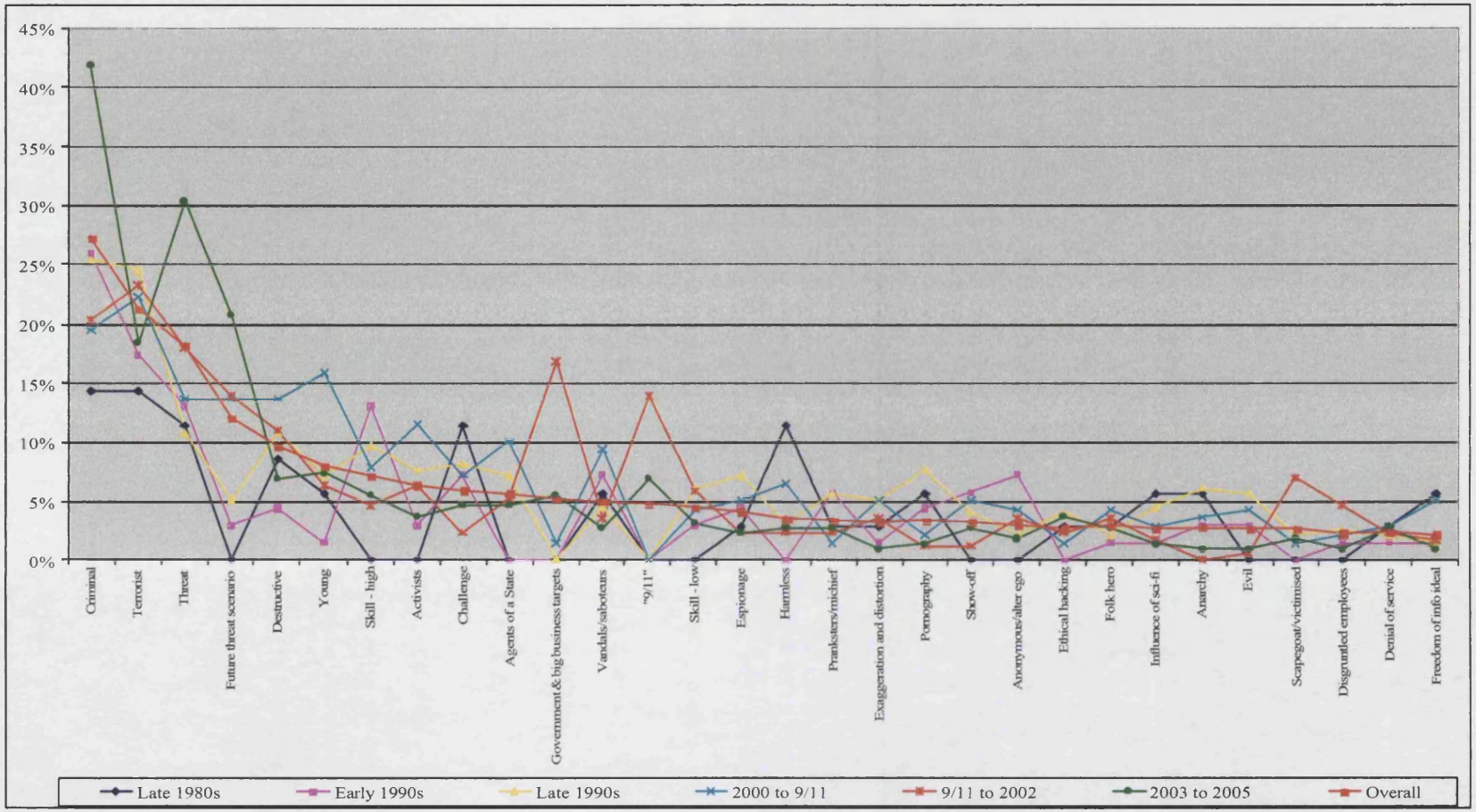


Figure 15 **Relative importance of *hacker* sub-codes: sub-codes as a percentage of total *hacker* primary codes for each time period**



In the late 1980s, the debate was mostly about the Computer Misuse Bill (later the Act of 1990) and what effect it might have on hackers. There was a prevalent view that, if hacking were criminalised in the Computer Misuse Act, it would:

> ... amount to 'a charter for blackmail' and will drive innocent youngsters underground and into the hands of serious criminals ...
>
> ... young people who hack innocently and for fun will be more inclined to listen to approaches from potential evil doers. ... 'Having committed one offence and been given a criminal record for innocent hacking, they may feel that they might as well get in a bit deeper.' *The Independent, 11 October 1989*

The same article went on to claim that companies would actually lose out if all hacking were criminalised because so-called ethical hacking (where the perpetrators tell companies how they breached security, thus allowing the company to patch the system) would equally be criminalised and because low-level hackers who had previously been informers in investigations into more serious crime would no longer be willing to perform that function. Computer product companies would continue to sell insecure goods because the security flaws would no longer be made manifest. At another level, it was argued that, whereas the *harmless challenge-seeker* once worked for society, within the system, as a kind of informal, external bug-hunter, he would now work against society, turning to the 'dark side' because society did not have the vision to incorporate him into the system. In other words, call a hacker a *criminal*, and that is what you will have. A clear example of labelling theory and deviance amplification in practice.

However, this argument did not prevail and hackers were criminalised. Only a part of the debate is found in this corpus, but the reason it occurs at all is that it was the first time hackers were labelled *terrorists.* In the long-running debate heralding the introduction of the Computer Misuse Act 1990, Emma Nicholson MP made a series of claims, including:

> ... 'I am very concerned that the key minister, who has not been brought up in a computer environment, may not have grasped fully the fearsome nature of computer terrorism,'... *The Times, 24 October 1989*
>
> ... no 'special case' consideration can be retained for the hacker. Those 'innocents' who claim immunity must realise that they stand in the company of the international terrorist and industrial blackmailer. *Letter to The Independent, 30 December 1989*

There was no suggestion at this stage that terrorist groups such as the IRA were resorting to hack attacks to supplement their conventional methods. In the late 1980s, the term 'terrorism' was used simply to add drama to the discussion about computer-related crime. Yet Nicholson seemed taken with her own rhetoric, including a vague

reference to Dutch and German extremists' use of "computer-derived information to bomb oil refineries and [destabilise] government actions" (*The Independent, 30 December 1989*). She was effectively the first in a long line of high-profile claims-makers to use cyberterrorism scenarios as an effective tool in arguing for extensions of social control.

The early 1990s saw an upwards trend in the scale of reporting of hackers. Similar views were expressed as to *criminality*, and the *terrorist* issue tends to be introduced to add impact to the claims being made.

> The hacker and the virus programmer embodied the popular notion of computer crime in the 1980s, and they are still the most widely known criminal acts in computer technology. ...
>
> ... His prospective list ranges from the annoying to the fraudulent, and includes small computer theft, desktop forgery, digital imaging piracy, voice and electronic mail terrorism, fax graffiti attacks, electronic data interchange fraud, and placement of unauthorised equipment in networks. *The Times, 3 April 1992*

However, there was still the pervading sense that, although these individuals were *criminals*, they were disruptive *vandals and saboteurs* more than dangerous, and still motivated by the *challenge* rather than base financial gain. That view started to change from the mid-1990s and a more serious brand of *criminality* came to the fore.

> The type of the computer criminal of the day before yesterday was the American Kevin Mitnick, an overweight, myopic prodigy who hacked into some of the most elaborately protected systems in the US ... Having got into these sacred cyberspaces, he did no harm - but he frightened the wits out of the corporations concerned, and was sent to gaol in 1988. ...
>
> But the new breed of cybercriminal is no juvenile meddler; he has very clear goals. Often helped by vulnerable young nerds, he hacks into companies to steal sensitive information of every description: hospital databases, credit reference agencies, tax files and files in newspaper offices have all been ransacked for potentially valuable information. Those behind the ransacking include firms conducting industrial espionage, detectives investigating for clients, and rival newspapers hoping to scoop a scoop. *The Independent, 13 October 1996*

Experts claimed that:

> 'There's a real shift in desire to attacks for personal, financial gain.' *The Guardian, 22 May 1997*

Concern was so high that the G8 held a conference on computer crime and hackers became the subject of political debate at an international level.

> When world leaders meet to discuss the greatest threats facing the human race, they normally talk about things like weapons of mass destruction, irreversible climate change, drugs and famine. But when the representatives of the G8 economic powers met in Washington this week, they added a new danger to the list: international computer crime. ...

> ... If the G8 ministers had been looking for an event which would underline both the scale of the problem and the difficulty of dealing with it, then such a thing occurred even as they met. On Monday night, hackers broke into the most popular Internet search engine, the California-based Yahoo! website, and threatened to explode a deadly virus 'bomb' into each of the 17 million computers which have visited the site in the past month. *The Guardian, 12 December 1997*

The transformation of the hacker into a dangerous *criminal* was well advanced, so much so that the transformation was itself the subject of press comment:

> The transformation of hackers in the public imagination is almost complete. The term, which once described pioneering West Coast programmers laying the foundations of the electronic frontier, now conjures up obsessive criminals hunched over terminals attempting to extract cash from banking systems. *The Guardian, 12 December 1997*

As the new Millennium turned, there was a dip in the portrayal of hackers as *criminal* as the focus moved over towards hacker as *terrorist*. This view had been propounded previously, but became more important at the turn of the century. This will be discussed further in Section 2.

Finally, in the period 2003-5 there was a huge increase in the proportion of quotations portraying hackers as *criminal* and a corresponding dip in the portrayal of hackers as *terrorist*. This huge increase in the *criminal* sub-code appears to be due partly to widespread reporting of, first, a number of notorious hacking court cases and, second, a number of notorious virus attacks. The court cases involved Simon Vallor, a virus writer; Joseph McElroy, blamed for sparking a nuclear panic by hacking into a US weapons laboratory; and Gary McKinnon, accused of scores of hacking offences in the US, some around 9/11, and facing extradition proceedings from the UK. The main viruses commented on during this period were SQL Slammer, Blaster, Mydoom, Sasser, Bagle and Netsky. However, the high levels of the *criminal* sub-code in the 2003-5 period also had much to do with the rather paranoid reporting of the *threat* from *criminal* hacker.

The view of the hacker as *threat* is the third most frequent in the corpus. This ties in neatly with the next most popular category: *future threat scenario*. There is some overlap between the two sub-codes, but the *future threat scenario* refers to a very specific form of claim, where the condition perceived as a threat has not yet materialised, it is merely predicted. Hacker as *threat* takes a much more general form and relates to threats from a condition which exists and is ongoing, the threat of information theft, for example. As Figure 15 highlights, hackers have always been perceived as posing a *threat* to society, whereas the *future threat scenario* was not applied to hackers until the early 1990s and has risen in significance since then. In both

cases, promotion of these views has peaked in the period 2003-5. 30% of all references to hackers in this period viewed them as a *threat* and this is explained by a massive increase in reporting of security vulnerabilities, mostly in a business context. The terrorist angle does not usually feature in these quotations.

> Businesses are failing to protect themselves adequately from crippling internet threats and computers are more vulnerable to cyber attack, new research shows.
>
> The study, conducted by Symantec, a provider of internet security services, also reveals that a sharp increase in the number of flaws in software is enabling computer hackers to take advantage of the weakness. *The Times, 3 February 2003*
>
> ... the survey found that 97 per cent of businesses rated security issues a matter of great or some concern, with terrorism, computer hacking and animal rights extremism being seen as the major threats. *Mail on Sunday, 7 November 2004*

The use of the *future threat scenario* has risen steadily since the early 1990s so that, for the period 2003-5, it featured in a fifth of all references to hackers. This, more formalised, view of the hacker as threat characterises new technology or security flaws as vulnerabilities which hackers might exploit.

> Technicians at the US software giant Microsoft are working flat out to prevent a new security threat that could this week give criminals access to computer systems used worldwide by banks and governments. Flaws in Microsoft software allow hackers to use replica internet banking sites to empty customers' accounts. *The Business, 13 June 2004*

Quotations featuring the *future threat scenario* often allude to the terrorist angle, the most common form being, 'If hackers can do this, terrorists might, too'.

> Security concerns are now growing in the wake of the recent virus attacks. The Windows systems that run on most personal computers are under threat from the new generation of worm viruses. The latest type of virus also presents an added security threat. A worm virus can be used to exploit weaknesses in Microsoft's operating system to take over control of the machine or deny legitimate users access. In today's climate, governments are increasingly aware of the opportunity this could potentially offer terrorists. *The Business, 19 October 2003*
>
> Millions of people risk having the personal information stored in their mobile phones stolen by a hi-tech electronic eavesdropping device, experts warned yesterday.
>
> It would enable paedophiles, terrorists and industrial spies to hack into handsets without the victims even realising. *Daily Mail, 15 April 2004*

Characterisations of hackers as a *threat* or a *future threat* tend to be highly depersonalised, the arguments flowing from what is technically possible, rather than what is humanly probable. This phenomenon has strengthened in recent years and there is no sign of abatement in the near future.

The other attributes of hackers featuring prominently in the frequency list presented in Figure 14 build a picture of a group of *destructive* youngsters, who have high levels of *skill* in their chosen activity, which they pursue chiefly because they find it *challenging*.

They are often seen as *vandals or saboteurs*, but might just as easily be *political activists* or *agents of a state*, either friendly or hostile. Hackers commonly *target government and big business* – the peak in the period 9/11 to 2002 is explained by a rash of 'hacktivist' activity and the indictment in the US of British citizen Gary McKinnon on hacking charges. Less often, but still significantly, they are seen as harmless *pranksters/mischief* makers, who exist to *show off* to their peers their dubious achievements.

Clearly, the overall reporting of hacker behaviour tends to the negative. There are some positive attributes higher up the frequency table, notably the views that hackers are *highly skilled*, see what they do as intellectually *challenging* (with the tenacity that implies) and are mostly *harmless*. However, positive attributes are more often towards the bottom of the table. Hackers are less often seen as *folk heroes*, *victimised* by society and used as *scapegoats*. '*Ethical hacking*' exists, but is less frequently reported, as is the widely held belief amongst hackers that *freedom of information* is an ideal.

Although the issue of *pornography* features reasonably high on the list, it is rarely claimed that hackers are closely associated with pornography. The links made in the press tend to be weak, such as "On the Internet, we are all at risk from hackers, pornographers etc". The association is deliberate, but stops short of actually confounding one with the other.

> But freedom is indivisible, and the open, unregulated nature of cyberspace offered opportunities not just to decent folks like you and me but also to unsavoury characters - money-launderers, tax dodgers, pornographers, paedophiles, hackers, virus-writers, terrorists and the like. *The Observer, 13 May 2001*

Because hackers are predominantly seen as *young*, perhaps it is possible that there is something of a taboo at work here. Whilst it is acceptable to claim that youngsters are engaging in an activity they find *challenging* but which is, nevertheless, *destructive*, there is a reluctance to claim that children are accessing *pornography*.

On the other hand, it is interesting to note what is not present: drugs. There were only four references to hackers and drugs overall. A search for references to *hackers* and *drugs* in close proximity (within 10 words of each other) revealed only 36 references in all UK national press articles in the Lexis-Nexis database. This compares with around 7000 articles citing hackers in total. Even the image of hackers as cannabis-smoking nerds does not seem to have permeated the press significantly. Rather, challenge, adrenaline, black coffee and junk food are seen as the drugs of choice for hackers.

> The Coffee Wars play up one of the computer hacker's most liberally served stereotypes; that they are nocturnal mammals whose penchant is for sucking strong cups of coffee as they raid sleeping computers. Hackers are also portrayed as being loners, sartorially inelegant, messy and lovers of spicy food. *The Times, 14 July 2001*

During the secondary coding process, the sub-code *character/appearance attributes* was applied every time a description of a hacker's character or appearance was encountered. This sub-code does not appear in Figure 14 since its purpose was to mark passages in which specific hackers or groups of hackers were described, as opposed to the usual references to hackers in the abstract. The adjectives used in the descriptions were collected and are presented in Figure 16, where they have been grouped, like with like. *Group 5* contains three attributes which are of a threatening nature, but each of these attributes was ascribed only once or twice in the entire corpus. This group aside, an entirely different picture emerges. The hackers described have addictive personalities (*Group 1*) and tend towards the juvenile in character, childish fantasists who are not popular with their peers and are particularly unsuccessful with girls (*Group 2*). This is a definitively male stereotype. These boys are meticulous and persistent with their hacking, tending to the reclusive and totally dedicated to the exclusion of all else. They will share information generally, but rarely cooperate in any given attack (*Group 3*). They are sometimes portrayed as brave but, more often, as having bravado, bragging about their skills (*Group 4*). Appearance-wise, hackers are often viewed as geeky, pasty-faced, with long hair and unshaven faces. They may either be chubby with junk food, or skinny with a wired look from too much caffeine. They will often wear either spectacles or branded shades, several body piercings and dress either entirely in black or in urban skateboarding gear (*Group 7*).

What does not appear in descriptions of individuals or specific groups of hackers is any reference to them being *dangerous* criminals or terrorists. Hackers such as the infamous Kevin Mitnick may be considered to have had the power to "blow up the world" (The Observer, 4 September 1994). But their supposed dangerous powers are eventually mitigated by the portrait painted in the press. Mitnick has spent time in prison for his hacking, but he was ultimately drawn as an addict who could not help himself, and a modern-day Robin Hood who exposed the flaws in Big Business. Despite his incredible skills, he would never have caused real harm, we are told. Unlike the black-and-white images painted of hackers in the abstract, individual hackers tend to grow out of their offending behaviour, and this is very much reflected in the media coverage:

Figure 16 **List of character/appearance qualities attributed to hackers**

Character	*Group 3*	*Group 4*	**Appearance**	*Group 6*
Group 1	anoraks	bravado	*Group 7*	bespectacled
addict	attention to detail	brave	geeks	thick glasses
nuts	dedicated	*Group 5*	pasty-faced	Oakley shades
obsessive	persistent	malevolent	chubby	body piercings
Group 2	little cooperation for attacks	neo-Nazis	slightly built	dressed in black
childish		S&M enthusiasts	goatees	skateboarding gear
cowards	share information		unshaven	
fantasist	lonely		long-haired	
playground reject	loners		ponytails	
hyperactive imagination	no life		sad	
ridiculous	reclusive			
unsuccessful with girls	need to get out more and meet some girls			
young				
	vain			

> [Computers set up for an experiment in PC security] were then intensively monitored by a team of experts which included Kevin Mitnick, the guy once regarded by the US government as the world's most dangerous hacker and now gainfully employed as a security consultant. *The Observer, 5 December 2004*

Similarly, Londoner Gary McKinnon is currently wanted in the US for hack attacks on the US Defense infrastructure around the time of 9/11. His offences are real, yet McKinnon is painted as a deluded soul who thought the Americans were hiding proof of alien life and was caught searching for that proof. He now lives in fear of what the Americans might do to him.

> He said: 'I am walking down the road and I find I cannot control my own legs. I'm sitting up all night, thinking about jail and what they might do to me. An American jail. And remember, according to them, I was making Washington inoperable immediately after September 11.
>
> ... 'I am only a little nerd.' So how did this jobless techno-geek with a fondness for science fiction and alien invasions find himself at the centre of a plot so bizarre that even the most gung-ho of Hollywood directors would reject it out of hand for being too fanciful? *Daily Mail, 16 July 2005*

All these attributes in Figure 16, when taken together, describe in detail the geeky, computer-obsessed, socially-inept, teenage stereotype which most people have in mind when they imagine a hacker. The importance of this finding is that it demonstrates that distance between a claims-maker and the subject of his hostility is key. When viewed individually, hackers are just geeks and, although disruptive, are not particularly harmful. Only when viewed as an amorphous group do hackers become the subject of the more worrying associations with dangerous criminality and terrorism. It will become plain below that all traces of humanity are erased when the *terrorist link* is described in the press.

2. THE TERRORIST LINK

The primary code *terrorist link* (n=657) was applied to all quotations in which a link was made between terrorism and hackers or the use of technology. This included all references to 'cyberterrorism'. There is some overlap with the sub-code *hacker as terrorist* (Figure 14) so that 139 quotations were coded with both *terrorist link* and *hacker as terrorist*. As before, a secondary coding process was undertaken to establish sub-codes for the primary code *terrorist link*. The quantitative results of this process are set out in Figures 17 and 18.

The striking feature of these results is that the *future threat scenario* is by far the most popular method of introducing the *terrorist link*, and it has become increasingly popular over time. In the absence of any concrete evidence in support of cyberterrorism, the

Figure 17 **Cumulative frequency distribution of *terrorist link* sub-codes by time**

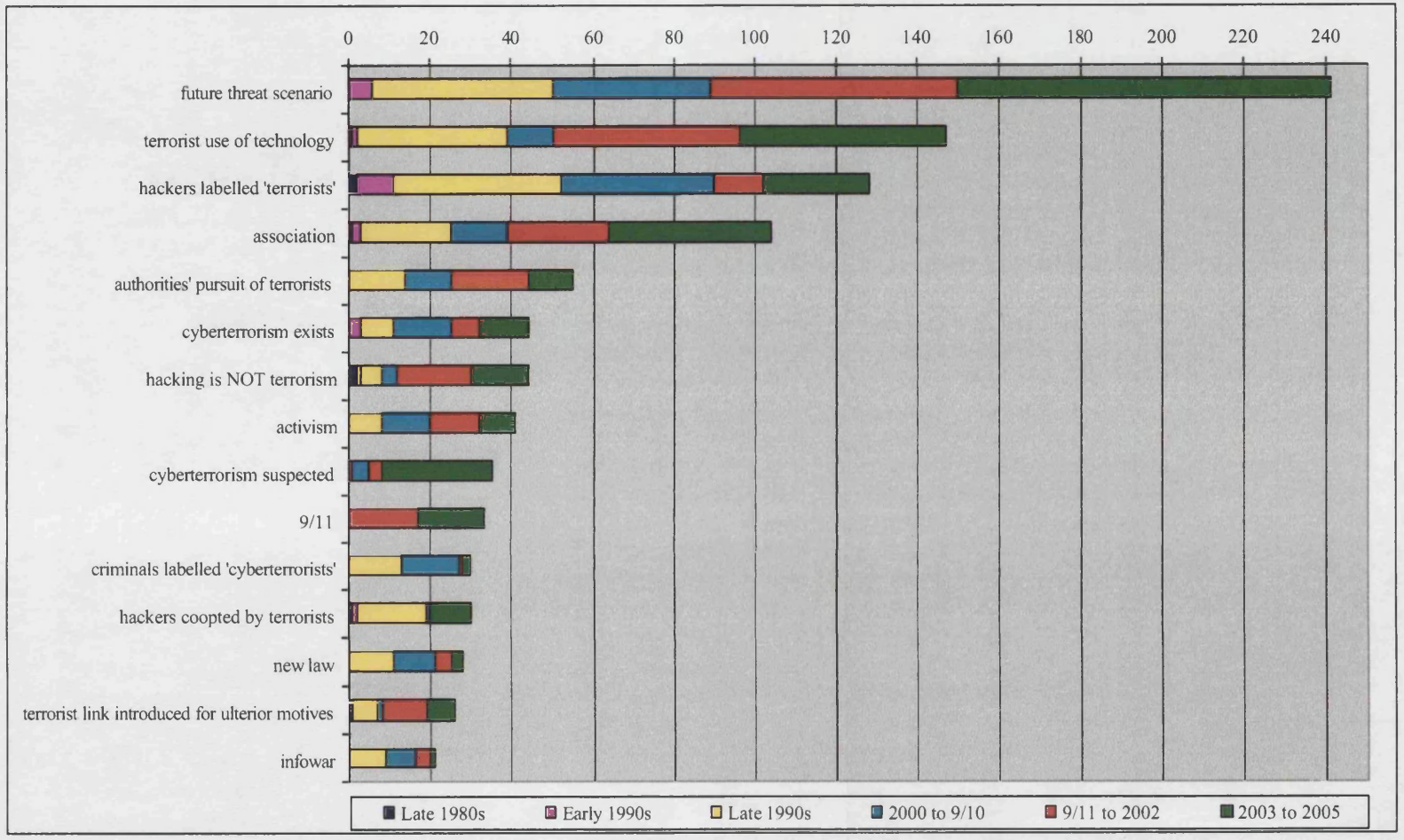
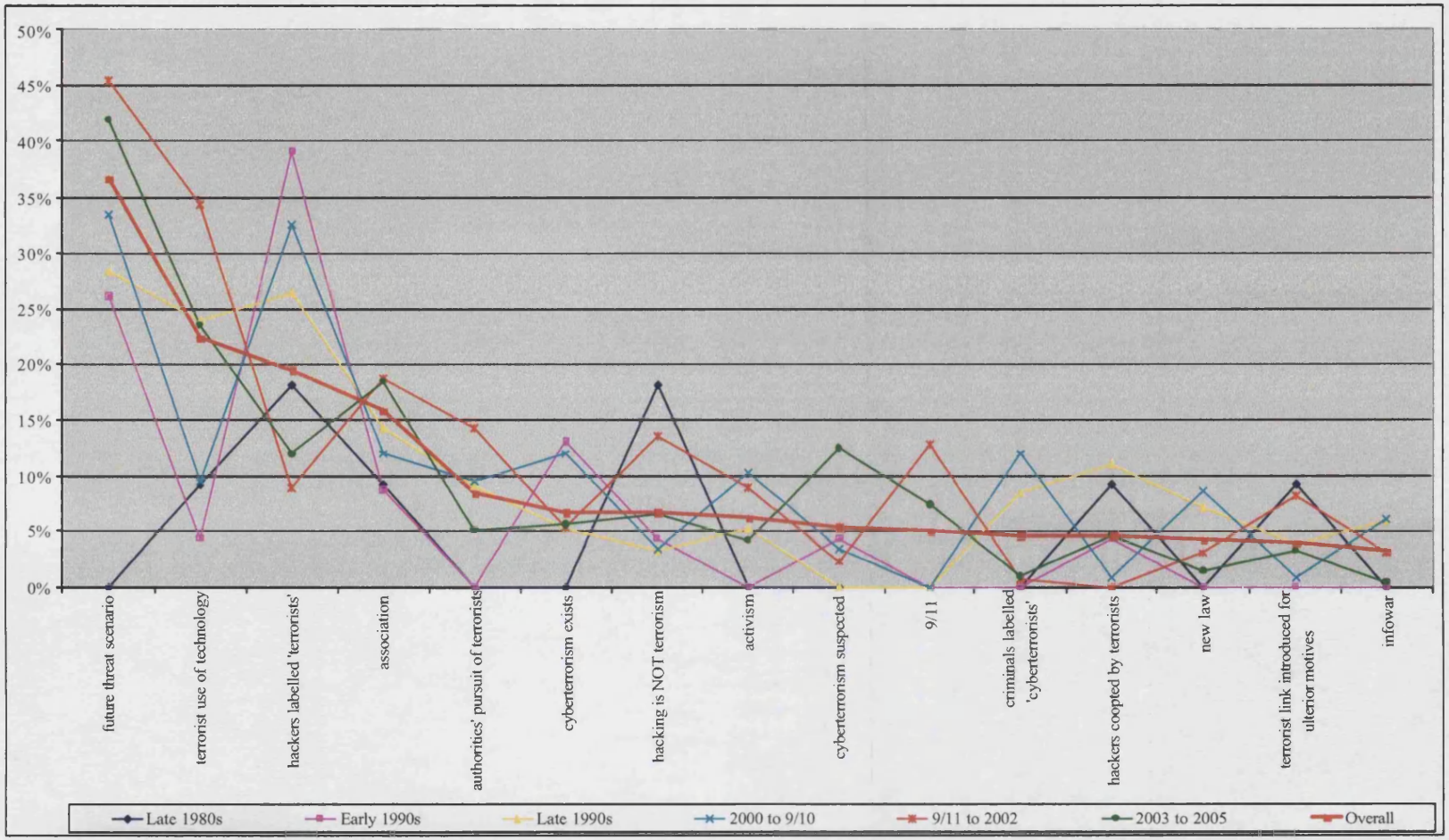


Figure 18 **Relative importance of *terrorist link* sub-codes: sub-codes as a percentage of total *terrorist link* primary codes for each time period**



majority of claims resort to this mechanism. The *future threat scenario* was not used in the press in the late 1980s, but started to appear in the early 1990s, during which period over one quarter of the *terrorist links* were made in this manner. Since then, there has been a fairly even increase in the use of the *future threat scenario* to a level of 42% for the period 2003-5. As might be expected, there was a peak of 46% following the 9/11 attacks. There was a pervasive sense of vulnerability which led society to look in all directions for possible attacks. Vulnerabilities brought about by dependence on technology were a common theme:

> The seriousness with which governments are taking all kinds of terrorist threats on the internet - including attacks by computer hackers - was further illustrated by one of the first US Congressional hearings following the tragedy, which focused on cyber attacks.
>
> At the hearing Joseph Lieberman, the Democrat senator from Connecticut who chairs the committee, said: "Our enemies will increasingly strike this mighty nation at places where they believe we are not only dependent but where we are unguarded. That is surely true of our cyberspace infrastructure today." A further hearing will take place tomorrow. *The Daily Telegraph, 21 September 2001*

It was also postulated that terrorists might use virus attacks to cause major economic damage, with phrases such as 'infecting systems with a lethal virus' sitting at odds with pure economic loss, but emphasising the deadliness of the perpetrators.

> E-commerce minister Douglas Alexander yesterday ordered internet security to be stepped up. He warned web experts from MI5, the MoD and GCHQ that increased vigilance was needed as terrorists could inflict major economic damage by bankrolling rogue computer hackers and infecting systems with a lethal virus. *The Mirror, 27 September 2001*

The use of disaster scenarios was widespread, with apocalyptic possibilities being peddled by those tasked with ensuring public safety.

> In the worst case, cyber-terrorists could open floodgates in dams or poison water supplies with sewage.
>
> Earlier this year, Ronald Dick, head of the FBI's National Infrastructure Protection Centre, expressed fears that attackers might cut power to hospitals and police radios after a conventional attack to maximise casualties.
>
> "Is that an unreasonable scenario? Not in this world. And that keeps me up at night," Mr Dick said. *The Daily Telegraph, 23 August 2002*

In the subsequent period, 2003-5, focus turned from the immediate aftermath of 9/11 towards the Gulf War. *Future threat scenarios* envisaged cyber-attacks from Islamic extremists as part of the insurgency.

> Terrorist groups may try to infiltrate the computer systems of some of Britain's biggest companies, government departments and emergency services if a war is launched against Iraq, the Home Office has cautioned.

> Stephen Cummings, director of the National Infrastructure Security Coordination Centre (NISCC), said key IT systems were under threat of cyber attack by Islamic extremists. *The Times, 20 February 2003*

As noted above (Chapter 6, Section 2.2 (c)), these attacks never materialised and politicians parried neatly with a subtle change in rhetoric: 'It may not have happened yet, but it will ...'.

> Even if the risk of cyberterrorism during the war was overstated, the threat of a serious attack by a rogue nation or a terrorist group remains very real, according to US government agencies. *The Guardian, 24 April 2003*

The *future threat scenario* at its most powerful, and useful.

On the other hand, there is significant evidence that terrorists make use of technology in the sense meant by Conway (2002). This is reflected in the number of quotations with the sub-code *terrorist use of technology* (n=147) which are spread over the whole time period covered by the corpus. There are many references to terrorists communicating by email, using the Internet for posting and gathering information and propaganda, and planning terror campaigns on computers, and these references peak, as one might expect, in the period 9/11 to 2002. None of this amounts to true cyberterrorism, although it is often represented as such in the press, as this example referring to the Bali bombing exemplifies:

> Headline: 'BIN'S FIRST CYBER BLAST'
>
> FBI investigators fear the outrage was al-Qaida's first cyberwar attack. Defence specialists believe Osama bin Laden fanatics planned and executed the bombing using computers. The masterminds could even have detonated their devices from thousands of miles away, possibly Pakistan or Kashmir. The CIA have established that bin Laden ran many of his earlier operations over the internet. An indication that an attack on Bali was planned came after the US Defence Department found hackers in Islamic former Soviet republics had tried to break their codes. *Daily Star, 15 October 2002*

The third most significant mechanism used to introduce the *terrorist link* is the relabelling of existing groups or social phenomena as 'cyberterrorist'. There are a number of sub-codes which refer to this relabelling process. The first is *hackers labelled 'terrorists'* (n=128) which refers to all instances where ordinary hackers have been labelled 'cyberterrorists' or very closely identified with terrorist activity with no obvious justification other than a desire to make a story more eye-catching. Figure 18 shows that the *labelling* of hackers as terrorists was very popular during the 1990s when cyberterrorism was still a relatively new concept and arguably had greater impact. However, as time went on, *terrorist use of technology* took over from *hackers labelled 'terrorists'*. This signals an interesting shift in emphasis so that the trend seems to be moving away from the ascription to hackers of terrorist motives towards terrorists being

ascribed technology skills in their own right. The mechanism of *labelling* hackers as terrorists is still important:

> James Adams, chief executive of Infrastructure Defence, which collates and provides information on cyberspace threats, says: "Hackers are a new form of terrorist. You can bring a country to its knees. It is a unique weapon. Things are getting exponentially worse." *Sunday Times, 4 April 1999*
>
> Is hacking a constant threat? I have been targeted by cyber-terrorists. It has mainly been by neo-Nazi groups and Islamic fundamentalists. *The Guardian, May 8, 2003*
>
> Last month was the worst-ever for computer terrorism, when the SoBig Virus helped cause business to lose £22 billion globally, say experts mi2g. *The Mirror, September 2, 2003*

However, it should be contrasted with the increasingly popular reporting of *terrorist use of technology* which leans towards terrorists becoming 'cyberterrorists' in their own right:

> "The battlefield is being played out in cyber space where the terrorists have used the Internet to indoctrinate, train and co-ordinate deadly terror attacks.
>
> The terrorists have become more sophisticated by linking up with cyber criminals to infiltrate the computer systems of major corporations as a means of stealing money to fund terrorists' activities.
>
> "The main threat we face is cyber terrorism which has the potential to destabilise our entire economy and information technology networks." *Sunday Express, 30 October 2005*

Next, there is the use of *association* (n=104), which can be considered a method of relabelling in that its aim is to associate two ideas (in this case hacking and terrorism) so closely that they are eventually confounded. Sometimes the association is unintentional, though none the less effective for that, but very often it is deliberate.

> Now an IT conference at Cambridge has heard how "terrorism, cyber-vandalism, other criminal activity, natural disasters and situations yet to be encountered can destroy supply chains and businesses". *The Guardian, 25 June 2003*
>
> On the plus side, Linux received a boost last week when it passed a security certification required by the US Defense Department. This enables it to be used on mission-critical computer systems, ensuring that these are safeguarded against hackers and cyber-terrorists. *The Business, 10 August 2003*

Association is often found in the context of a *future threat scenario* in which, for example, a newly discovered vulnerability might be exploited by hackers and terrorists.

> ...as Britain becomes more reliant on computers, vital Government systems, including those in the health service, air traffic control and defence, are becoming more and more vulnerable to malicious attack.
>
> "An attack could come from individuals such as hackers, criminals or terrorist groups who might benefit from seeing our business disrupted," said a Home Office spokesman. *The Independent, 7 February 1999*

There are two further types of relabelling which were found to be significant in the corpus. The first was the relabelling of *activism* as cyberterrorism, very often political activism taking the form of defacing websites and posting propaganda.

> Israeli prime minister Ariel Sharon looks on grinning at a swastika daubed over the Stars and Stripes.
>
> This is the latest shocking example of the surge in political cyber terrorism that's hitting Western businesses.
>
> "Hundreds of similar propaganda images are uploaded on to online servers every week by pro-Islamic hacker groups protesting at the prospect of war with Iraq, Israel-Palestine and other Islamic - interest issues," says a spokesman for digital risk specialist firm mi2g. *The Mirror, 27 February 2003*

The final type of relabelling is where *criminals are labelled 'cyberterrorists'*. This almost exclusively relates to attempts by criminal groups to extort money, usually from financial institutions, by threatening to attack their computer networks. This is not cyberterrorism and does not even qualify as true cybercrime, in the sense that no unauthorised access to the system is actually achieved, only threatened.

> City of London financial institutions have paid huge sums to international gangs of sophisticated "cyber terrorists" who have amassed up to Pounds 400m worldwide by threatening to wipe out computer systems. *Sunday Times, 2 June 1996*

The importance of all these cases of relabelling is that they create 'cyberterrorism' out of existing phenomena which have not previously been considered to have any links with terrorism. Thus, the net is widened to include hackers, activists and criminals under the umbrella of cyberterrorism. Attacking from the other side is *terrorist use of technology*, a mechanism which attempts to create 'cyberterrorism' by adding the ingredient of technology to existing terrorist activity.

Turning to the sub-codes with lesser frequencies, sometimes the *terrorist link* is introduced through reports of the *authorities' pursuit of terrorists* (n=55). The corollary of *terrorist use of technology* is that the authorities can also use technology as an investigative tool:

> E-mail and telephone data has proved vital in the fight against Al Qaeda. *Sunday Times, 16 June 2002*

It also follows that encryption and other technologies which might hinder these investigations meet resistance from law enforcers on the basis that it would hinder the tracking of terrorist activity across the Internet.

> So why don't the FBI and other law-enforcement agencies in America (which generally decides what happens on the Internet, whether we like it or not) like encryption? Perhaps they think it will make it harder to catch terrorists. *The Independent, 30 September 1997*

Elsewhere in the corpus, it is baldly claimed that *cyberterrorism exists* (n=44) as a matter of fact or, alternatively, that *cyberterrorism is suspected* (n=35) to lie behind a particular attack.

> "In fact, even prior to last summer the proportion of attacks by cyber terrorists from pro-Islamic sources was negligible. Now we estimate that at least 15 per cent of digital attacks are from these sources. A range of pro-Islamic groups are working together to target the infrastructures of countries such as the UK and the US." *The Times, 24 February 2003*

> Terrorists are feared to be behind an alarming rise in hackers' attacks on top-secret government computer files. *The News of the World, 24 March 2002*

> It seems too much of a coincidence that New York and then parts of London and Kent were plunged into darkness.

> Could the power cuts in these two major cities have been caused by people hacking into the computers that control the power grid by any chance? And, if so, are these people criminals anarchists or terrorists? *The Mirror, 4 September 2003*

Finally, to the question of which messages are present, but attenuated. The most important message of all is that there has never been a publicly verified cyberterrorist attack, although this does not preclude the possibility that the government and security services are in possession of classified information to the contrary. There are other, related issues, such as the fact that it is exceptionally difficult, if not impossible in most cases, to cause death or serious injury through a remote hack, however talented the hacker; that causing economic loss probably does not inspire terror in the sense meant by 'terrorism'; and that the weight of considered academic and professional opinion still considers that, if terrorists are interested in cyberterrorism at all, the threat is probably not imminent. Data drawn from the corpus demonstrate that claims that *hacking is not terrorism* (n=44) are present but not common. They were most prominent in the late 1980s when many experts were trying to argue that criminalising hackers would lead youngsters who were not causing significant mischief to turn to more harmful activities. There was another peak in such claims after 9/11 when cyberterrorism was suspected to be behind various attacks and law enforcers and industry insiders were forced to spell out that this was ordinary hacking, not terrorism.

> The involvement of FBI cyber-crime agents and the Office of Homeland Security raised the spectre of terrorism, but the expert consensus - echoed by Mr Fleischer - was that the attack was far more likely to be the work of conventional hackers, possibly young computer users seeking a wider stage for rivalries hatched during online gaming sessions. *The Guardian, 24 October 2002*

> Bank of Ireland confirmed that material originating from Russia had been sent out in its name. It said, however, that it understood the emails were harmless and it was unaware of any terrorist link. *Sunday Times, 27 October 2002*

Although it is not widely reported, there is a reaction to the process of relabelling described above, and the sources for such comments tend to be journalists, experts and hackers themselves, keen to debunk the more sensationalist claims being made.

> Many experts also say ... those who launch virus attacks are more likely to be 'cyber-vandals' not 'cyber-terrorists'. 'Terrorists make targeted demands and like a high degree of control over their operations. A supervirus is more likely to be the brainchild of a spotty adolescent than some terrorist mastermind.' *The Observer, 7 May 2000*

To summarise, the most significant factors linking terrorism to information security issues are use of the *future threat scenario* and discussions of *terrorist use of technology* as if this amounts to cyberterrorism. In both cases, the technology itself is often at the heart of the claims, not just its human operators. The next section sets out perceptions of the technology which emerge from the corpus.

3. DEMONISATION OF THE TECHNOLOGY

The sub-codes derived from the secondary coding of the *technology* quotations and the quantitative findings are set out in Figures 19 and 20.

Overall, *technology* is most often discussed in the corpus in the context of the *future threat scenario*. The proportion of quotations devoted to such discussions has increased with each successive time period, demonstrating its increasing importance as a rhetorical mechanism. For the period 2003-5, 42% of all references to technology in the corpus involved a *future threat scenario*. In the great majority of cases, a new technology or development is described and predictions are then made about how it might be used or abused by criminals or terrorists.

One recent case highlights the tensions created by the development of technologies which can be used for both good and bad purposes. Calls were made in the US for anonymising software to be banned on the grounds that it might be used by terrorists. Its author claimed it was intended to promote free speech.

> The Senate commerce committee in America recently called on the US government to legislate against such technology because terrorists might employ it. ...
>
> ... The programmer says his software will permit the anonymous publication and consumption of information on the internet, making it impossible for governments, especially repressive regimes, to restrict information. "My hope is that it will be more difficult for undemocratic countries to censor their citizens' access to information through the internet," he said. *Sunday Times, 7 August 2005*

To call for a complete ban on such software appears an extreme reaction by most standards. Very often, the future threat scenario is combined with other claims about

Figure 19 **Cumulative frequency distribution of *technology* sub-codes by time**

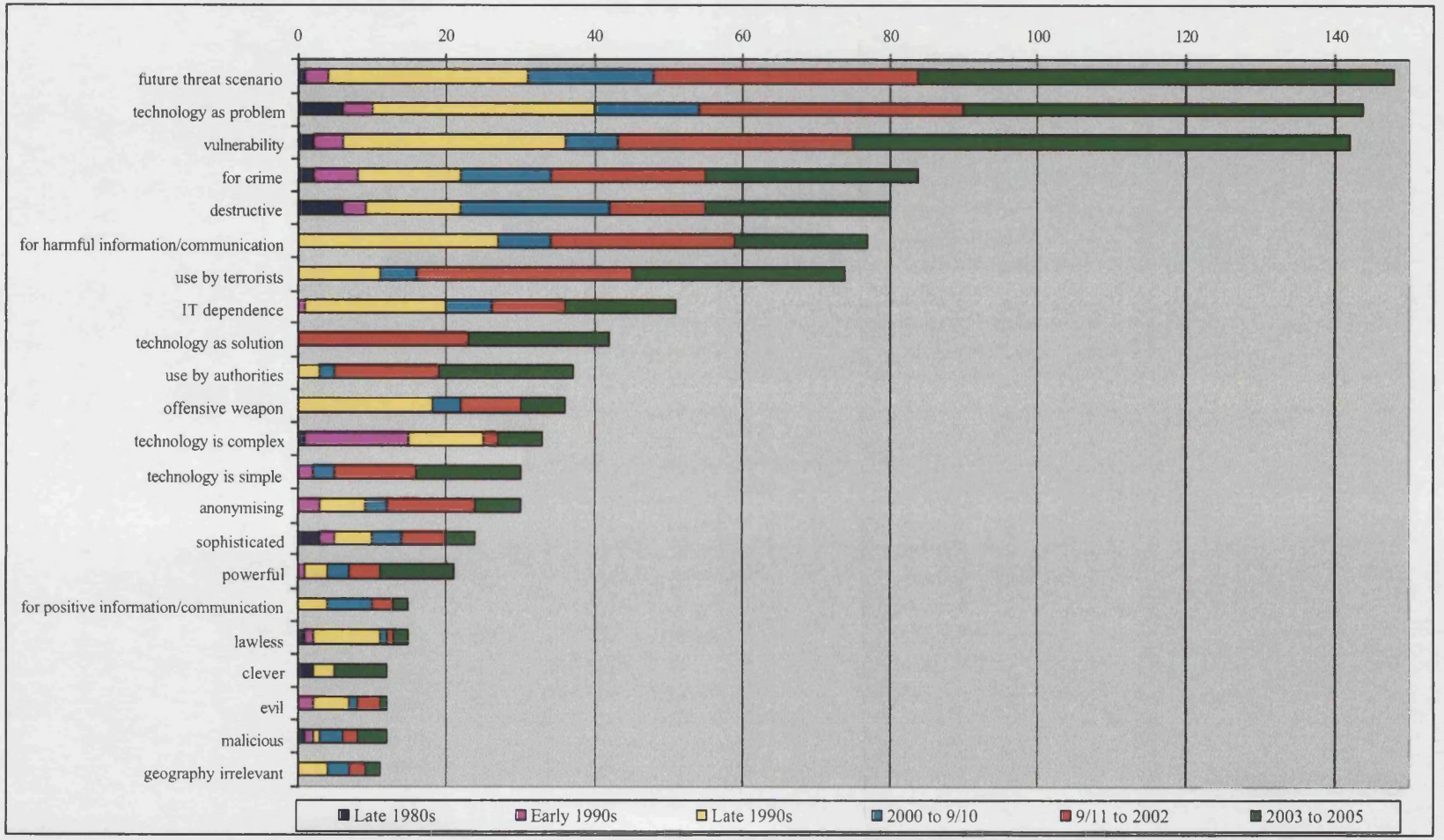
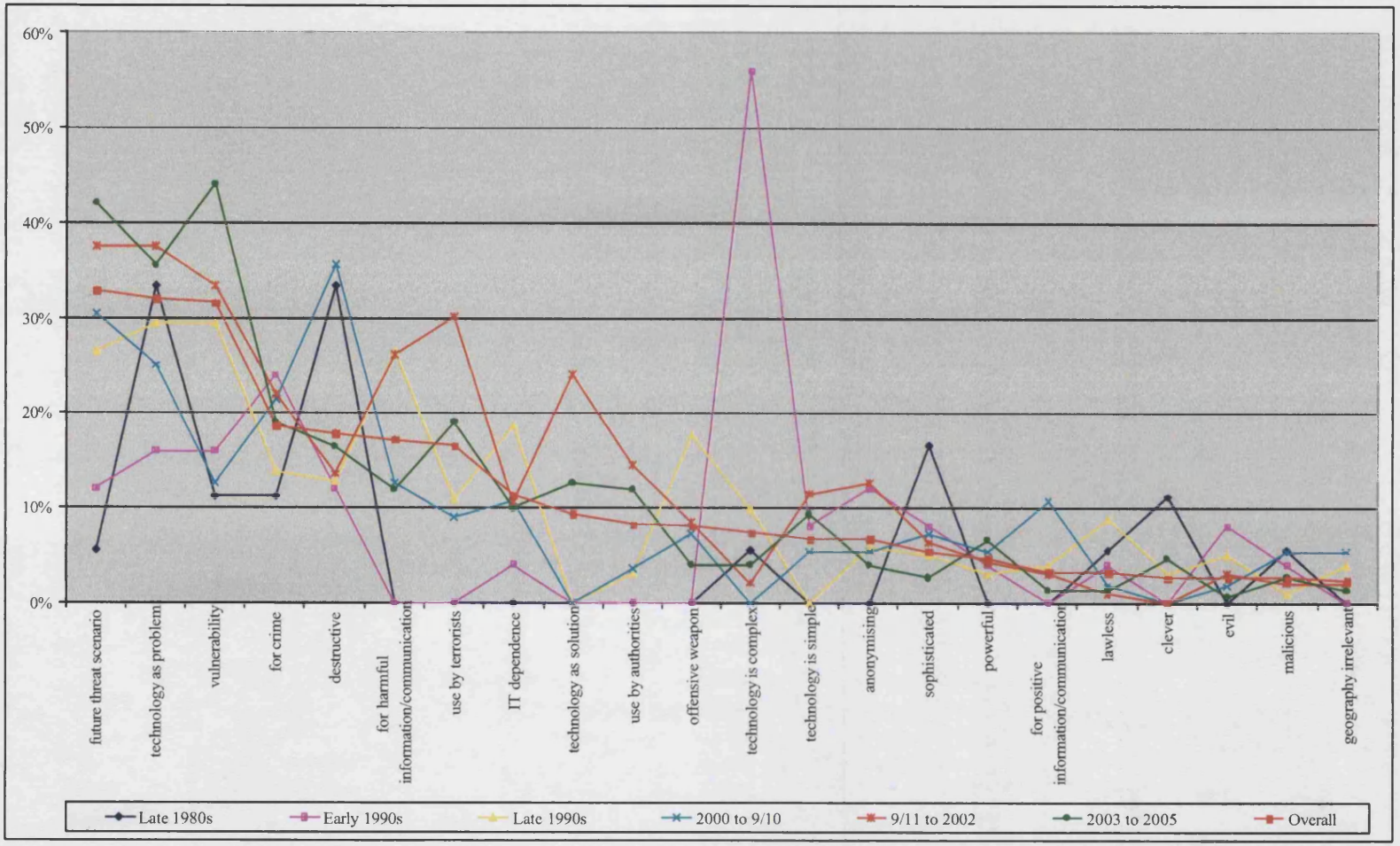


Figure 20 **Relative importance of *technology* sub-codes: sub-codes as a percentage of total *technology* super-codes for each time period**



technology. In these examples, the focus is on *vulnerabilities* 'caused' by technology and by *IT dependence*, both major themes discovered in the corpus.

> The attack clearly shows the weakness that Microsoft's growing monopoly causes to a country reliant on computers: if every computer runs the same operating system, all will have the same flaws, and a lone cyber-terrorist could seriously disrupt communications. *The Independent, 5 March 1998*

> [Richard Clarke, chairman of the US President's critical infrastructure board] argues that we should be worrying about how to protect our critical systems, rather than where the next attack will come from. Every new technology is a potential target for cyber-terrorists. ... "Now, if you're a terrorist, the first thing you might want to do before an attack is take down the 911 system," says Clarke. *The Guardian, 20 February 2003*

Thus, *technology* itself becomes the focus of claims about cyberterrorism since the arguments are really about what the technology makes possible, rather than evidence of the motivations of terrorists. In the same context, *technology* has been portrayed as an *offensive weapon* which, when combined with the *future threat scenario*, makes for a very potent image:

> The West's intelligence agencies are bracing themselves for the use of what they have dubbed "weapons of mass disruption": when terrorists take up cyberwarfare, hacking into the West's key control systems, all of which are computer-dependent. *The Independent, 13 October 1996*

In the context of this corpus of data, the portrayal of technology is overwhelmingly negative. Representations of *technology as problem* were over three times more numerous than *technology as solution*. The former code was applied to quotations which cast technology as problematic, creating a *vulnerability*:

> Technology may be able to help the industry, but it also introduces security threats. One former airline insider, who asked not to be named, says there are two critical weaknesses in airline technology that could be exposed by terrorists and criminals. *Independent on Sunday, 23 September 2001*

...a means of attack:

> Experts say there is growing concern that terrorist groups are trying to use the internet both to communicate and to launch cyber-attacks on US and British companies and government bodies in order to create chaos. *Sunday Times, 14 October 2001*

...or a channel for crime:

> The Net was hailed as the ultimate communication tool. But the Superhighway has fast become the tool of pornographers, pimps, drug-sellers and burglars. *Daily Mirror, 28 November 1995*

> But freedom is indivisible, and the open, unregulated nature of cyberspace offered opportunities not just to decent folks like you and me but also to unsavoury characters - money-launderers, tax dodgers, pornographers, paedophiles, hackers, virus-writers, terrorists and the like. *The Observer, 13 May 2001*

The representations of *technology as solution* tend to go hand-in-hand with *technology as problem*. The view is that, where one technology creates a difficulty, another technology can be used to address that difficulty. It is noteworthy that this view does not become prevalent in the corpus until after the 9/11 attacks, underscoring the technical approach to security which characterised that period.

> "[The airlines' e-booking system] is wide open to abuse," said one airline insider. "Sophisticated criminals can easily create fake IDs and hack into the internet."...
>
> But ... security threats could be thwarted by the technology of one US firm, Visionics, which makes software that can recognise facial features and patterns. It can also be used both to check the authenticity of an identification document and to check a passport photo with the face of the person holding it, removing the possibility of human error.

Amongst the quotations on *technology*, there is also significant emphasis on a phenomenon discussed in Chapter 6: that technology, especially the Internet, is a double edged sword and, if it can be *used by terrorists*, it can also be *used by the authorities* hunting them down.

> So is the internet a boon to criminals and terrorists everywhere? Surely what is sauce for the terrorist goose is sauce for the police gander, so to speak. Just as the internet offers new opportunities for communication among terrorists, so it represents a major step forward for law enforcement. *The Guardian, 22 November 2001*
>
> James Bond-style technology is used to track criminals and terrorists but now texts are proving vital evidence in securing convictions. *Sunday Express, 18 April 2004*
>
> The government is excited rather than alarmed by what technology can do. It sees utility, not danger, in each opportunity to increase its surveillance. If more of our movements and purchases are logged, it will help the police to fight crime. *Sunday Times, 3 July 2005*

The well-rehearsed arguments about the use of technology *for crime* and for *destruction* are familiar and have been used in relation to hackers for years. They are only relevant to the issue of cyberterrorism when combined with the *future threat scenario*: terrorists might use the Internet for fraudulent purposes in order to raise funds; or they may use viruses to destroy the systems on which the Stock Exchange relies. On the other hand, the use of technology (usually the Internet) for *harmful information/communication* is very pertinent to terrorism generally. In the words of one journalist:

> The internet has been getting some bad publicity recently because of its presumed role in helping terrorists perpetrate the September 11 atrocities. In addition to using the internet to communicate, the shadowy network of terrorists supposedly hid encoded information in image and music files. The message is that the internet is complicit in the planning and execution of evil crimes. The implication is that the internet itself is evil - even more than mobile phones, which the terrorists almost certainly also used. *The Guardian, 22 November 2001*

It is often reported that terrorists use email and websites to communicate with each other and with sympathisers.

> Al Qaeda cyber terrorists are plotting over the internet to launch a suicide attack on Britain's HMS Ark Royal using a speedboat packed with explosives. *Daily Star, 14 March 2003*
>
> Al-Qaeda chiefs are circulating plans to British extremists for a bomb designed to evade airport scanning machines, writes Adam Nathan.
>
> The instructions for the "invisible" bomb are among thousands of Al-Qaeda files in a secret online repository discovered by computer hackers and passed to MI5. *Sunday Times, 26 October 2003*

There is also the issue of availability of information on techniques, such as how to make bombs or viruses, which is not so much communicated from A to B, but is generally available to all. It is almost axiomatic that, whatever you want to know, you can find the information on the Internet.

> But you don't need the coding abilities of a Netsky or Mydoom author to create basic viruses. Virus-writing websites and toolkits make it easy for any malcontent to create their own computer plague. *Mail on Sunday, 16 May 2004*

In contrast with the prevalent view of technology being used for *harmful information/communication*, its use for *positive information/communication* is much less widely reported. When it is, the *positive* aspects are usually presented as the flip-side of the *harmful* ones. This is a good example of how positive messages about technology have been attenuated in the context of the debate on cybercrime and cyberterror.

> The Net was hailed as the ultimate communication tool. But the Superhighway has fast become the tool of pornographers, pimps, drug- sellers and burglars. *Daily Mirror, 28 November 1995*
>
> The trouble is, not only does the Internet allow the mass distribution of ideas, but it can also bolster their plausibility.
>
> The Web is establishing a democracy of ideas on a scale unimagined by previous generations. With plans to connect all schools to the Internet, the issue of controlling access to 'undesirable' sites is being hotly debated. *The Guardian, 17 July 1997*

IT dependence was a theme which occurred reasonably often, signifying a preoccupation with the *vulnerabilities* brought about by such dependence. There is a very real sense of unease which arises when manning the physical boundaries of a nation against attack is no longer enough and people begin to perceive that there are other ways to attack a nation on its home soil and that the geographic location of the enemy is irrelevant.

> For a country relatively free from terrorist attack inside its borders, news of this vulnerability comes as a shock. The more computerised, the more technologically

> sophisticated they become, they are being told, the more vulnerable they are to cyber-terrorism. *The Independent, 22 October 1997*
>
> [President Clinton] has ordered the military to develop its own information warfare capabilities to respond to such attacks. But [Congressman] Weldon, describing dependence on computer systems as "the Achilles heel of developed nations", said this is not enough. *Sunday Times, 25 July 1999*

Finally, this sense of unease is highlighted again in the quotations coded with *technology is complex* and *technology is simple.* When technology is viewed as *complex*, the argument generally goes that it is possible for certain, gifted individuals to invade our information systems secretly, spy on us, modify, destroy or steal our data and then withdraw leaving no trace that they have ever been there. They are able to do this because they have mastery of these arcane systems and ordinary people do not. There is a strong feeling of lacking control over the systems society depends on due to their complexity.

> New generations of viruses are taking advantage of the complexity of the latest computer operating systems to spread software devices that propagate themselves, hunt down information of interest and send it wherever they want via the Net. *The Guardian, 18 March 1999*
>
> A teenage hacker narrowly escaped jail yesterday after sparking a nuclear panic by keying into the computer system of a top-secret U.S. weapons laboratory.
>
> Joseph McElroy was a 16-year old schoolboy when he bypassed the electronic security with sophisticated software he had developed and nicknamed Deathserv. *Daily Mail, 3 February 2004*
>
> ... as CCTV becomes driven by computers instead of videotape, any expert hacker will be able to find his way into your private security system. Even now, if you have a webcam, then (if you can be tricked into downloading some Trojan-horse software) you can be watched in your home by an outside hacker, whether a private individual or a state agency. With broadband, people leave their computers on all the time, which means the possibility of 24-hour surveillance within the walls of your own house. *The Times, 14 May 2005*

The stand-out result from all the coding on technology is a massive peak in the early 1990s in the presentation of *technology as complex*. During this period, 56% of all references to *technology* described it as *complex* (Figure 20). Whilst there is no single reason for this finding, it seems to be borne of a feeling of helplessness, of being out of control. This was also the period when hackers' skills were perceived as being at their highest (Figure 15) and it was not yet widely known that many hacking tools could be downloaded from the Internet – the view of technology being used *for harmful information/communication* had not yet registered (Figure 20). The perception was that hackers had the upper hand and their skill was such that they could do as they pleased without redress.

> 'The hackers are now so sophisticated that their knowledge is outstripping the technology designed to keep them out.' *Mail on Sunday, 14 February 1993*

But there was suspicion of computers themselves and the mood of the time is nicely captured in this quotation:

> Of course, computers being such complex machines, we should expect "and learn to live with" bugs and inconsistencies. In fact, their complexity, and the resulting unpredictability, is the source of a kind of cyber-superstition. Most of us still have no idea how computers function. All we know is that they can work some powerful magic; so powerful, who knows where it stops? Hence the chatter about mutant cockroaches living inside PCs and video display terminals which leak carcinogenic radiation. *The Observer, 11 April 1994*

Since the turn of the Century, there seems to have been a move away from viewing technology as *complex* to the view of *technology as simple*, that 'anyone can do it with cheap equipment and tools downloaded from the Internet'. This finding is supported by the corresponding rise in the view of technology being used *for harmful information/communication.* This chimes with the New Millennium paranoia which was so exacerbated by 9/11, the subsequent wars and civilian attacks. It also makes more compelling the argument that terrorists are able to and will perpetrate a cyber attack. If technology is still portrayed as being highly *complex*, this *future threat* argument becomes harder to make.

> [Due to a flaw in Internet Explorer] banks and governments are at risk from organised crime and terrorists. All the hackers need to break into any computer system running Microsoft's Internet Explorer is for a single user at an organisation to log on to the internet on Monday morning using Explorer. *The Business, 13 June 2004*
>
> ... in a chapter of his autobiography entitled "Hacking, Why Not?", the Bali bombings mastermind Imam Samudra directs readers to Indonesian-language sites for instructions on how to carry out online credit card fraud and money-laundering. These instructions are simple to follow: ... a consultant on international terrorism ... calls it "hacking for dummies", and adds that "in this day and age, you don't have to be an expert hacker to have a tremendous impact". *Sunday Times, 11 September 2005*

The point about simplicity is very often reinforced by claiming that 'even a child could do it'.

> Once the access point was identified it was relatively easy to log-on to the Government network. To prove how simple the process was we asked an 11-year-old boy to repeat it - he did. Our reporters were then able to monitor the flow of electronic data around Portcullis House. For example, every time an email was sent it registered on a box on our laptop screen. It clicked up 26 times in the time it took to turn the corner of the building in a car. *Sunday Mirror, 18 August 2002*
>
> And this [a DDoS attack on the 13 DNS root servers] was done not by some fiendishly clever piece of cracking, but by off-the-shelf techniques involving the penetration of unprotected machines all over the net (mostly running Microsoft software) and then using these zombies to flood the DNS servers with packets until each machine in turn was overwhelmed and unable to respond to legitimate requests. It's so simple a child could do it. For all we know, a child did. *The Observer, 27 October 2002*

Of the remaining themes found in the quotations on *technology*, there are two which bear special mention. Concern is expressed that technology can be used to ensure *anonymity* and this is often linked with the idea that the networked nature of modern information systems makes *geography irrelevant*, particularly where cyber-attacks are concerned.

> Triangle Boy works by allowing computer users to evade filters and firewalls - barriers used by governments, schools and corporations to restrict access to sensitive or unsuitable sites to authorised users only.
>
> The software also helps those attempting to enter sensitive sites secretly by foiling investigators' attempts to trace back any "break- ins" to the computer used and the country it is in. *Sunday Times, 14 October 2001*
>
> Like many of the sites used by Muslim groups to promote their cause in Chechnya, Kashmir and Afghanistan, the IOC's was set up using technological expertise in the UK. Creation of the websites follow a similar pattern with details deliberately spread around the globe in an attempt to conceal the identities of the people providing both the content and funding. *Independent on Sunday, 28 October 2001*

Once again, the ideas that terrorists might be able to communicate anonymously and attack without the need for physical proximity have caused much vexation to law enforcers and politicians alike.

Summary

There is one theme which cuts across the analysis of all three of the elements of cyberterrorism: the *future threat scenario.* In all cases, it is a highly significant mechanism used to create or highlight concern. The classic formulation highlights a new technology or the discovery of a new system vulnerability and predicts ways in which such things might be used by hackers and/or terrorists to threaten society in some way. This unites the elements of cyberterrorism and creates a sense of immediacy which surrounds the issue, generating concern about deviant groups which is not necessarily based on solid evidence.

There are significant processes of redefinition being undertaken. Hackers are relabelled 'cyberterrorists'; terrorist use of technology, whilst not amounting to cyberterrorism, is labelled as such; the technology itself is being re-examined in the light of *potential* uses by terrorists. One fact is certain: true cyberterrorism is not yet with us. Nevertheless, the cyberterrorist has already been defined into existence.

The next chapter will discuss the policies and mechanisms of social control which have been introduced in the name of combating cyberterrorism; consider whether the social reaction is proportionate to the scale of the threat; and examine the evidence as to how

and why efforts have been made to sustain concern about cyberterrorism over the last 20 years.

CHAPTER 8

FINDINGS: DISPROPORTIONALITY AND VOLATILITY

This chapter will assess the evidence relating to the final two ingredients of the attributional model of a moral panic: disproportionality and volatility. Section 1 will gauge whether it can be said that the subjective response to cyberterrorism is disproportionate to the objective threat. Section 2 will consider the extent to which there is volatility in the social dynamic. Although these two elements are not connected to the same extent as, say, concern and consensus, they are presented in the same chapter because the task in both cases is to draw together the threads of the evidence presented thus far rather than assessing exclusively new evidence.

1. DISPROPORTIONALITY

According to the arguments rehearsed in Chapter 3, it is scientifically defensible to measure subjective views against an objective dimension, in this case the levels of concern about cyberterrorism against an objective assessment of the risk. Moreover, it is possible to formulate objective propositions, even if they are couched in conditional and tentative terms. Where the existence of a threat is exaggerated and couched in absolute and alarmist terms, it is usually possible to counter that the probabilities of the threat crystallising are much lower than stated and the effects are unlikely to be as severe. Distortion may also be present in discussions of the causes and effects of cyberterrorism.

One further, practical problem must be addressed, a problem not discussed in the moral panic literature. It is all very well, it might be argued, for academics to assess levels of objective harm having, as they do, access to the very best and most up-to-date studies, theories and reasoning. Yet the subjective concern of the ordinary man is based on the information to which *he* has access. His concern should only be judged as disproportionate, therefore, if it is disproportionate in terms of the information available to *him*. The approach taken in this section, therefore, is to formulate objective propositions against which to measure subjective concerns, taking account only of information available in the corpus. This acknowledges that an average reader of a UK

daily newspaper has ready access to the information contained in the corpus in a way that he does not have access to the kind of academic or industry information referenced in Chapter 2. The question is still one of proportionality, but the focus shifts from objective standards derived from external scientific enquiries towards objective propositions derived from a critical analysis of the information presented in the corpus. This is on the basis that the reader of a UK national newspaper is able to apply critical reasoning to information in an article he reads (whether or not he does so is a moot point) because media reporting is not homogeneous and does provide alternative viewpoints which can be compared and contrasted, rather than accepting at face value the information presented. His hypothetical response will only be considered disproportionate if other information from the corpus and a critical approach suggests it is so.

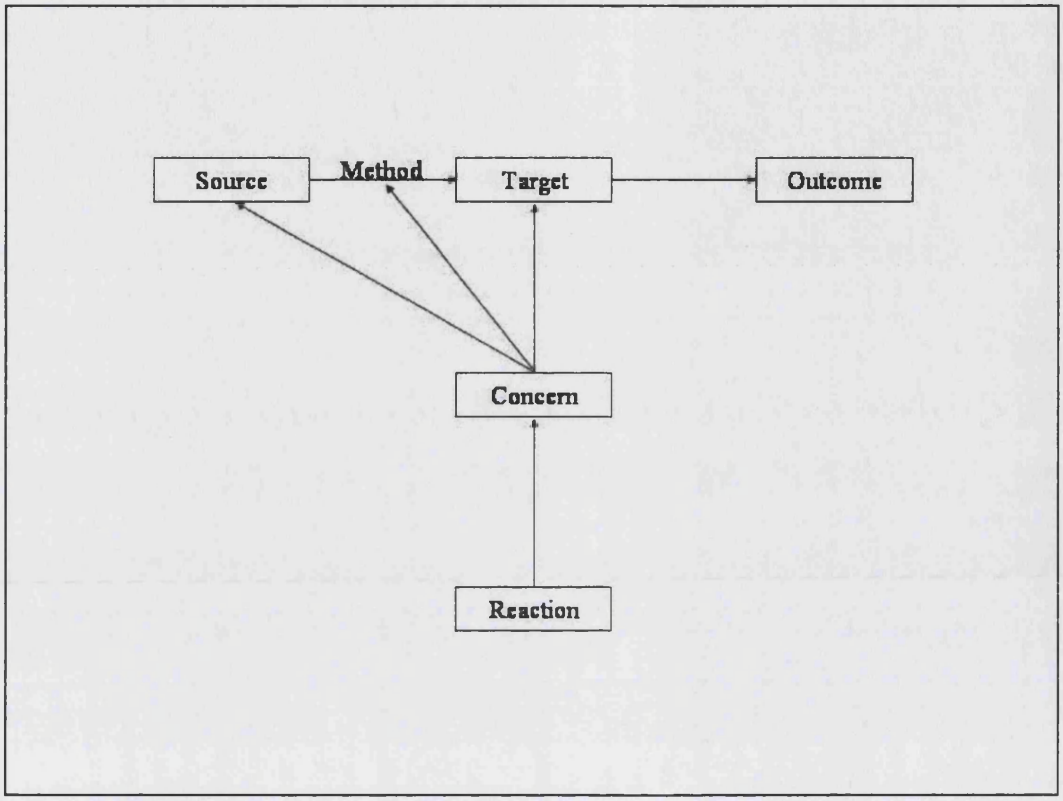
Certainly, many of the reactions represented in the corpus are the reported reactions of politicians, industry insiders, journalists and the like. Unlike the ordinary man, they do have ready access to other information and specialist advice. However, by reducing the analysis to the 'lowest common denominator', it is possible to argue that, for example, a politician who claimed that X is a serious threat should at the very least have realised that it was not as much of a threat as he was suggesting because of information readily available in the press. These are the grounds on which the ordinary man would be able to judge the politician's claim.

Concern about a cyberterror attack is often identified with a particular element of an attack (Figure 21). First, there is the concern about the source of the attack, in other words, those deemed responsible. Then, there are concerns about the method of the attack, the target of the attack, and its outcome. Finally, there is the high-level social reaction to the phenomenon. In each of these areas, it is necessary to identify where fear and concern exceed appropriate or proportionate levels and where causes and effects of deviance have been distorted (Critcher 2003: 151). At each stage, propositions can be formulated, based on the available evidence, against which the concerns noted in previous chapters can be measured.

A final note: generation and dissemination of figures fabricated or exaggerated by claims-makers is normally a very important feature of the dimension of disproportionality in a moral panic. In the case of cyberterrorism there are figures – generated by the information security industry, government and law enforcers and usually relating to hacking offences and quantification of damage – but they play a

relatively small part in a debate which is far more focussed on unquantifiable future threats.

Figure 21 **Anatomy of a cyberterror attack**



1.1 Source of attack

Claims that cyberterrorists exist, that hackers are turning to terrorism or that terrorists are turning to hacking are rife in the corpus and were detailed in Chapter 7. One fact is certain: there has never been a true act of cyberterrorism publicly reported, in the press or anywhere else, although it is always possible that such an attack has taken place but that the information has been kept classified by the government and security services.

> There's curiously little proof that al-Qaida or other terrorist groups are engaging in cyberterrorism. Robert Andrews, a congressional representative from the state of New Jersey and a member of the House select committee on homeland security, concedes that there is "no evidence on the public record" that any terrorist group has ever launched an attack on the information infrastructure of the US.
>
> It turns out that the vast majority of network intrusions and hacking attempts against US computers aren't the work of terrorists hiding out in caves along the Pakistan/Afghanistan border, or hackers in Russia or China, but originate within the US. One security firm estimates that 86% of all "security events" can be traced back to the US. *The Guardian, 24 April 2003*

Despite the claims that cyberterrorists exist, close reading of the material in the corpus reveals that there are no specific claims that, for example, al Qaeda have hacked into the British CNI or that the IRA have ever succeeded in committing an atrocity using

information technology alone. There are occasional claims that a terrorist group is behind a particular event, such as the electricity failures on 14 August 2003 in North America, but these are always exposed later as having been accidents or the result of hacks without terrorist motive. There is plenty of believable evidence that terrorists use technology but no evidence in the public domain of cyberterrorist attacks (Denning 2000). Claims by civilians that the latter have taken place are, therefore, likely to be wide of the mark unless they have privileged access to classified information.

> The CMA [Communications Management Association] asked 172 of its senior personnel to report on incidences of cyber-terrorism in their organisations. Anonymity was guaranteed, though many of the companies involved are household names. ... Thirty-two per cent admitted being the victim of cyber-terrorism. *The Guardian, 3 April 2001*

It is clear that the term 'cyber-terrorism' is used here to describe criminal breaches of security, and yet the claim is unequivocal: 32% of respondents have suffered cyberterrorist attacks. There is no shortage of such examples:

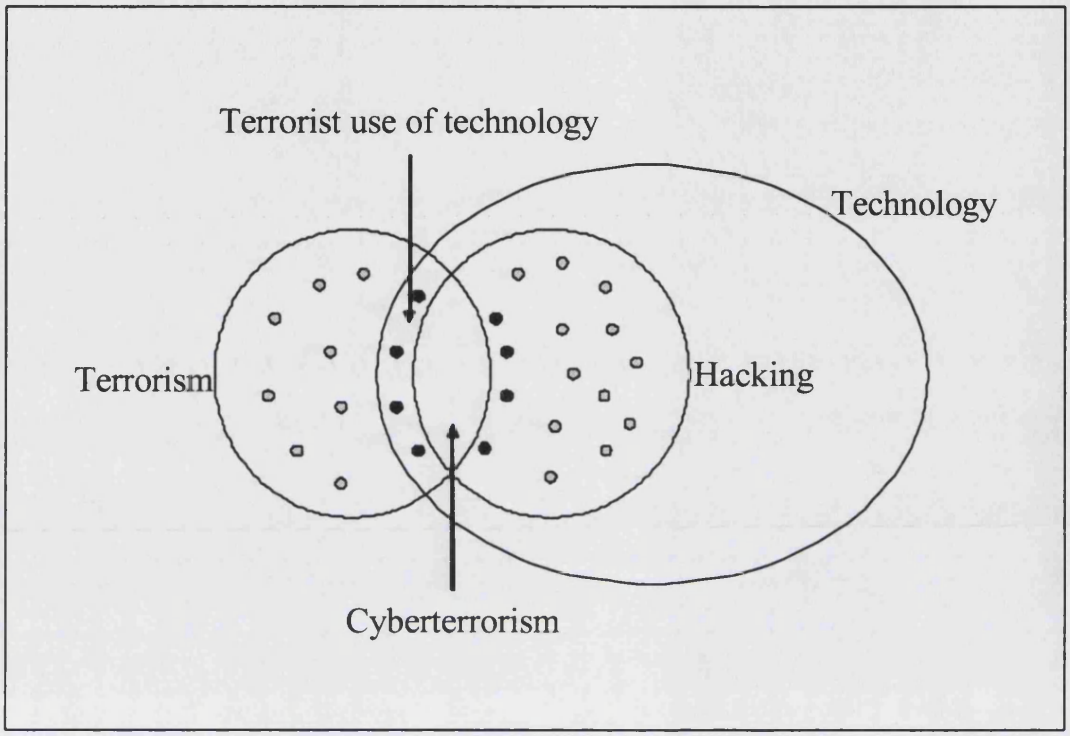
> There is now evidence that the cyber-terrorist net is widening to include a larger number of firms. According to Mi2G, there are 65,000 projected overt attacks for 2002, an increase on the figure of 31,332 for 2001.
>
> "This indicates terrorist groups are targeting smaller companies than before and are also focusing on attacking ISPs internet service providers , where a single penetration can take down 500 corporate websites," an Mi2G spokesman said. *The Business, 3 November 2002*
>
> In fact, even prior to last summer the proportion of attacks by cyber terrorists from pro-Islamic sources was negligible. Now we estimate that at least 15 per cent of digital attacks are from these sources. A range of pro-Islamic groups are working together to target the infrastructures of countries such as the UK and the US. *The Times, 24 February 2003*
>
> Cyber-terrorists have launched a record number of attacks on business and government computers. There were 20,182 attacks around the world in the first 20 days of May, breaking the previous monthly record of 19,658 attacks in January.
>
> A quarter of all attacks were the work of political or religious hackers protesting against Western policy in the Middle East. Systems in Britain, the USA, Germany and Argentina were the main victims, said digital risk specialists mi2g. *The Mirror, 23 May 2003*

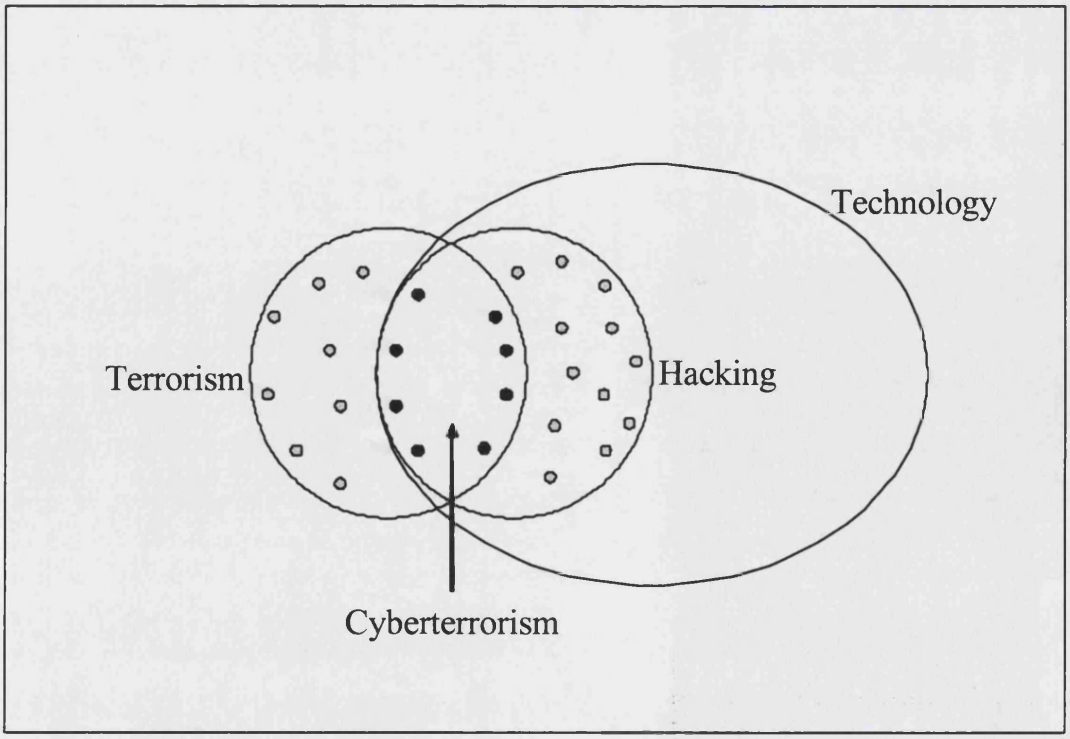
What seems fairly clear is that these are all false statements based on a redefinition of ordinary information security breaches as 'cyberterrorism'. Sensationalisation of the language in which the findings of surveys are expressed quite clearly leads to disproportionate levels of concern in the target audiences:

> It seems almost suicidal to connect a business to the internet, if the statistics for fraud, hacking and other computerised malice are right. The latest study says that 44% of UK businesses have suffered "a malicious security breach" in the past year. *The Daily Telegraph, 7 May 2002*

The false statements and exaggerations with respect to the source of cyberterrorism, that is, those deemed responsible, almost always comes down to net-widening through redefinition.

Figure 22 **The concept of net-widening**





The concept of net-widening can be considered using a Venn diagram (Figure 22): consider a set 'Terrorism' and a set 'Technology' with its subset 'Hacking', 'Cyberterrorism' being the intersection of all three. Applying the definition of cyberterrorism used in this study, the intersection is, apparently, currently empty as there has never been a publicly documented case of cyberterrorism. However, by attributing terrorist motives to serious hacking cases and by relabelling terrorist use of the Internet and other technologies 'cyberterrorism', some of the elements are drawn into the intersection. A similar argument has been made in relation to computer crime:

In fact, by altering the definition of computer crime you can make it as large or as small a problem as you wish. Computer security consultants, surprise, surprise, tend to favour wide definitions; hard pressed police forces can 'solve' the problem of computer crime by refining it out of existence. *The Guardian, 5 May 1988*It is not necessary to rehearse them again, but the findings set out in Chapter 7 demonstrate that net-widening is indeed prevalent on two levels. First, hackers are often labelled 'terrorist' in circumstances where there is no evidence of any terrorist motive or involvement (Figures 14, 15, 17 and 18). This is usually a rebranding exercise, as in this example relating to the Sobig F virus:

> Internet giant Microsoft said yesterday it is working with the FBI and the Secret Service to track down those responsible for this week's virus attack.
>
> Coming so soon after another point-blank virus attack on Microsoft last week, the Seattle-based firm is on red alert and fearing a co-ordinated attack on world commerce by so-called e-terrorists. *The Express, 23 August 2003*

In other cases, it is simply assumed that, of all the hackers in the world, some of them must be working for terrorists.

> Although al-Qaeda's ideology is simplistic, it seems to have access to sophisticated IT. One of the newest items of intelligence jargon is what some experts call "Hackint" - intelligence obtained from the penetration of information systems. According to a US presidential commission, the global population with the computer skills required for Hackint operations and other forms of cyber-attack against important Western targets has grown from a few thousand 20 years ago to about 19 million today. It would be naive to assume that none of them works for al-Qaeda. *The Times, 4 October 2001*

This may be true, but no firm evidence has been presented that terrorist organisations have teams of hackers working for them. Whatever the true position, the contention that 19 million individuals have the skills to execute targeted information raids of the type implied by the term 'intelligence' must be false. It is frequently claimed that tools are widely available on the Internet to enable individuals to construct various types of malware, but it is extremely unlikely that these tools could be used to gather the sophisticated intelligence necessary for a truly targeted and devastating attack unless the

operator were unusually skilled to begin with. There are few enough hackers with skills at this level (see father Section 1.2 below).

Second, terrorist use of technology for communication, organisation, fundraising through criminal activity, recruitment and propaganda is often labelled 'cyberterrorism' (Chapter 7, Figures 17-20). This is not an accurate use of the term and produces a disproportionate amount of concern by conjuring up visions of cyber-attacks which are simply not taking place. Even if terrorists are, for example, going one step further by creating and distributing destructive viruses – a proposition which has never been proved in public – this does not amount to terrorism.

> "Even something as serious as major outages that have been accidents - there's a reasonable argument that the 2003 North-East (US power grid) blackout was the result of a computer problem, but even if al-Qaeda were to do it, they would not call it terrorism - it's bad, it's expensive but no one would be terrorised." *Financial Times, 16 November 2005*

So, the argument goes, viruses do not inspire fear in a population or coerce governments into acting differently. Terrorist use of technology is a concern, as is anything which facilitates terrorist activity, but the level of concern it inspires should be proportionate to concern over other facilitators of terrorism, such as financial sponsors and training camps. With or without technology, terrorists will function just as other criminals do.

> But this does not mean that the Internet is full of bomb-making instructions. It is not. The same goes for hacking information, guides to lockpicking, sexually-explicit material, discussions of drugs, banned books, and anarchist literature. All are available online in roughly the same proportions as you'd find them offline. *The Guardian, 27 July 1995*

As well as the reclassification of existing activity as 'cyberterrorism' there is also, of course, the widespread use of the future threat scenario. This mechanism introduces high levels of concern in respect of conditions which have yet to arise. The issue of disproportionality arises precisely because these issues are a matter of pure conjecture. The fact that the majority of these scenarios are technology-centric – positing what might happen because technology permits, rather than focussing on the motivations and skills of hackers or terrorists – is central to an understanding of why the future threat scenario is so strong.

> Forget about missiles, bombs and outlaw militias armed to the teeth. The United States faces another threat that is invisible, but potentially even more lethal. According to a report delivered to President Clinton this week, the most powerful state in the world could be laid low by the flick of a cyber-terrorist's switch. *The Independent, 22 October 1997*

The allegation is that cyberterrorism is a simple matter, necessitating merely the flicking of a switch. It is argued that terrorists have hijacked our technology and are using it

against us in myriad ways, the next logical step from terrorist 'use' of technology being a cyberterrorist attack.

> Simon Barrett, director of the International Coalition Against Terror, said: "We are fighting an information war against Islamic terrorists who are manipulating and abusing our advancement in Western technology to undermine our way of life.
>
> "The battlefield is being played out in cyber space where the terrorists have used the Internet to indoctrinate, train and co-ordinate deadly terror attacks.
>
> The terrorists have become more sophisticated by linking up with cyber criminals to infiltrate the computer systems of major corporations as a means of stealing money to fund terrorists' activities.
>
> "The main threat we face is cyber terrorism which has the potential to destabilise our entire economy and information technology networks." *Sunday Express, 30 October 2005*

There is no evidence presented in the article to support such assertions: this is another example of the usual reasoning, being "It must be possible, so it will probably happen". It is arguable that such bald assertions can be presented as authoritative on the basis of a public lack of understanding of technology, a suspicion borne of the fact that its workings are invisible, that evildoers can hide behind it, that physical barriers are no longer sufficient to protect society from harm, all concepts found with relatively high frequencies in the corpus (Figure 19). If experts proclaim that a certain attack is possible, the argument goes, then a terrorist is bound to carry it out.

> In days gone by, people were not so much frightened of science, as oblivious to it. ...
>
> ... The pride and scorn for science, that saw most people through the 20th-century, is now giving way to fear. Why the change? Jargon and methodology, more than ever, are raising the wall between the cognoscenti and Everyone Else. After all, it is a truism that we fear that which we don't understand ...
>
> ... we have been plunged into brain-scrambling mobile phones, brain-gnawing prion diseases, contaminated foodstuffs, not to mention the underlying stealth of chemical and cyber-terrorism... Small wonder there is a simple knee-jerk to veto all this confusion and scary technology in one go. How can Joe Public, after a hard day at work, come home and be expected to tease out the pros and cons, weigh up the risks, consider all the implications, and differentiate the "yuck" from the reality. Wouldn't it be much easier to sit back in a past where everyone was 100% human, with their human values and understanding: the post comes three times a day, there are no mobiles, emails, or videos, perhaps no planes... *The Guardian, 10 April 2003*

It is, in part, this fundamental lack of technological understanding which may prevent the public from asking questions, leading to acceptance of otherwise tenuous claims. The fact that the threat is a *future* threat gives greater strength to the claims because, by definition, there is no evidence of the threat having crystallised yet, so it seems unreasonable to demand any. But even when strong claims are made – the Millennium Bug, widespread cyberterrorism prompted by the second Gulf War – and they subsequently fail to materialise, the vast majority of individuals persist in their mute

acceptance. It is claimed that "It didn't happen this time, but the threat is still strong..." and this argument still goes unchallenged.

> Even if the risk of cyberterrorism during the war was overstated, the threat of a serious attack by a rogue nation or a terrorist group remains very real, according to US government agencies. *The Guardian, 24 April 2003*

The true power of the future threat scenario lies in its ability to produce a level of concern disproportionate to the scale of the risk. The concern here is not with rigorous risk analysis and a careful presentation of the findings, but with those sensationalised statements based on pure conjecture.

> It is a chilling cyber-scenario as set out by Singapore government minister Ho Peng Ke. Instead of a backpack of explosives, he has warned - justifying new laws against "computer misuse" - a terrorist could create just as much devastation by sending "a carefully engineered packet of data" into the computer systems which control essential services, such as the power stations.
>
> The supposed menace of "cyber-terrorism" has become the subject of alarming predictions of this kind since September 11, most of them originating in the new sense of vulnerability felt in the US. The subject conjures an image of Dr No come back to life with supreme keyboard skills. In the words last year of US homeland security director Tom Ridge: "Terrorists can sit at one computer connected to one network and can create worldwide havoc." *The Guardian, 19 November 2003*

Certainly, it is possible, but is it really likely? There is no evidence presented that a cyberterrorist could "create just as much devastation" as a "backpack of explosives".

> After September 11, US cyber-warfare experts also found that users on Saudi, Indonesian and Pakistani servers had been studying US computer systems governing emergency phone systems, nuclear power stations, dams, reservoirs, water pipelines and gas storage facilities.
>
> "We were underestimating the amount of attention (al-Qaida was) paying to the internet," Roger Cressey, the chief of staff of the White House critical infrastructure protection board, told the Post.
>
> "Al-Qaida spent more time mapping our vulnerabilities in cyberspace than we previously thought. The question is a question of when, not if." *The Guardian, 28 June 2002*

The only certainty arising from this extract is that there have been attempts at breaching the information systems which control the US CNI, and some of them may have been successful. It is also clear that some of these attacks have originated from or been routed through Saudi, Indonesian and Pakistani servers. Does this really justify a claim that al Qaeda have been 'mapping our vulnerabilities in cyberspace" and that it is a "question of when, not if"? Such statements can, and should, be challenged, but they are not.

Interestingly, there are some who appear to believe their own hype. When a serious hack was discovered in US military systems, terrorists were suspected:

> Boffin Joseph McElroy sparked fears that World War Three was being started after he hacked into a top-secret US nuclear weapons installation.
>
> McElroy, aged only 16, developed his "Deathserv" software at his home in east London to crack the security shield of the US Department of Energy, which is responsible for the safety of America's nuclear weapons.
>
> In scenes reminiscent of the 1983 film WarGames, in which a computer whizzkid hacks into Pentagon computers, US officials thought they were under attack from terrorists. *The Express, 3 February 2004*

Considering that nearly all known culprits for this type of hack have been young men or, as here, boys, announcing the start of World War Three seems a strangely disproportionate response.

1.2 Method of attack

There are two major aspects to the element of disproportionality when it comes to discussing methods of cyberterrorist attacks. First are the claims that risks from cyberterrorism are high in circumstances where the realities of conventional terrorism make the possibility of cyberterrorism pale into insignificance. Second are the claims, already touched on, that the existence of certain technologies will automatically lead to terrorist exploitation.

Dealing first with the cyber vs. conventional terrorism debate, ample evidence has been presented in previous chapters of claims that cyberterrorism is a real and growing threat:

> Howard Schmidt, vice-president of the President Bush's Critical Infrastructure Protection Board, believes terrorists are searching for ways to use privately owned assets such as power grids, financial systems and telecoms networks to wreak havoc.
>
> Mr Schmidt told The Times yesterday that more than 80 per cent of infrastructure deemed "critical" for society to function properly is privately owned, and much of it is vulnerable to cyber attack. *The Times, 15 October 2002*

But the degree of concern actually warranted by the threat of cyberterrorism must surely be far less than the concern merited by the reality of conventional terrorism. Common sense and even a tenuous grasp of current affairs imply that conventional terrorism is a present danger in the Western world, one against which the vast resources of the state are ranged and for good cause. On the other hand, information security breaches are also a real concern, but the perpetrators here are criminals, not terrorists. It is entirely right that an entire industry exists to service this need for information security which, incidentally, has the merit of protecting against cyber attacks from criminals and terrorists alike.

> Mark Rasch, former head of the US Justice Department's computer crime unit ... says many of the strategies that corporations are adopting to protect themselves against ordinary hacker attacks will also serve them well if terrorist organisations such as al-Qaeda strike. *Financial Times, 16 November 2005*

When compared with the real and pressing problems of conventional terrorism and cybercrime, the high levels of concern about the possibility of cyberterrorism expressed by politicians, law enforcers, industry, experts and the media seem disproportionate.

> But Bruce Schneider, a leading cryptographer and founder of Counterpane Internet Security, points out that [cyberterrorist] attacks are yet to happen. The threat is somewhat overlooked because it is also overblown, he suggests.
>
> "I think it's largely a media creation. We know what terrorism is - it's planes flying into buildings, it's not that you can't get your e-mail," he says. *Financial Times, 16 November 2005*

In very simple terms, there are many, more immediate threats to worry about. There are several reasons for this. Firstly, a targeted conventional terrorist attack is far easier and more accurate than its cyber equivalent.

> But Hollywood-style hacker scenarios such as those outlined in the latest James Bond movie are far removed from reality. At least, that's according to the people who should know: the hackers themselves.
>
> As hackers and security consultants gathered last week for Dublin's Hivercon conference, a newer and simpler argument was aired: that it is far easier to be a real-world terrorist than a virtual-world one. *The Guardian, 5 December 2002*

As one experienced hacker claims:

> "Cyberterrorism is a catchy phrase and seems to be a hot topic. I'm not saying that a hack could never lead to someone's death, but it's much easier for a terrorist to throw a knapsack of poison into a reservoir than to do something remotely with a computer," he says.
>
> "If I knew George Bush was going into hospital and would be on a life support system, conceivably I could interrupt the power grid or hit the back-up batteries in the middle of his operation. But most of these systems already have a lot of safeguards, mainly just to prevent simple accidents." *The Guardian, 5 December 2002*

Secondly, due to the type of security protecting some of the most critical systems, insider assistance would often be required for a targeted attack.

> Thieme argues that the true cyber threat does not come in the traditional form of the disaffected hacker located in a remote country, but the insider - the guy who already knows all the passwords and works inside the system. *The Guardian, 5 December 2002*
>
> ... it's difficult to see how serious damage could be caused by someone not equipped with insider knowledge - they've got to know about the technical aspects of the system they're trying to damage."
>
> This is why Peter Sommer, of the London School of Economics Computer Security Research Centre, dismisses the idea of an impending "electronic Pearl Harbor". The number of people in government who know the sort of sensitive security information that terrorists would need is very few, he says. *The Guardian, 20 February 2003*

It would be possible and relatively easier for a terrorist group to plant an insider or persuade an existing insider to work for them, and the mechanics of any targeted cyber attack suggest that there ought to be more concern about this threat from insiders,

criminal or terrorist, than about external cyberterrorists. Yet the faceless outsider remains the focus of society's fears.

Next to cyberterrorism, cybercrime is a genuine and far more pressing problem because of its sheer scale. Most information security breaches are of a routine nature and are easily countered with appropriate security systems, frequent updates and patches, although genuine concern is warranted about the extent to which many organisations fail to execute routine updates.

> "I am amazed at the number of staff who automatically open every attachment they're given," he says. If you're not expecting an attachment, [Jack Clark, Network Associates] advises, always phone or email the sender to check they meant to send it. "Make back-ups of everything and have as few email addresses in your address book as possible. Most importantly, make sure you continually update your anti-virus software." The first rule of combat, after all, is to be properly armed against the enemy. *The Guardian, 5 June 2000*

Hackers good enough to commit a theft or attack CNI using purely electronic means are relatively rare and do not form a significant part of the problem, although they are high-profile. Once again, the levels of concern expressed in this regard are disproportionate to the scale of the problem.

> Most attacks are by "graffiti writers" on websites, [Mike Barwise, Computer Security Awareness] says, and then come the less common hacks into systems for financial fraud or other personal gain. Rarest of all are what he calls the "uber-hackers": the one or two per hundreds of thousands of hackers who are good enough to hack into government systems and yet cover their tracks. "That isn't prevalent,"... *The Guardian, 20 February 2003*

The second main issue of concern in terms of methods of attack relates to technology itself. Two of the many examples relate to demonisation of the Internet and the case of encryption. It is an incontrovertible fact that technology is used in the vast majority of cases for legitimate purposes. Yet the mere prospect of illicit use, particularly of the Internet, seems to have some concerned parties reaching for the draft legislation:

> One of the more galling moments in media coverage of the Internet came in early reports of the Oklahoma City bombing. Someone on Sky News showed a file called The Terrorist's Handbook that he'd picked off the World-Wide Web ... Demands poured in from, among others, US Senator Dianne Feinstein, that information about making bombs be banned from the Internet - even though the information is available from many other sources. *The Guardian, 27 July 1995*

> Over 4,000 people turned up to hear International Telecommunications Union secretary general Dr Pekka Tarjanne argue that a little regulation may be a good thing when the Internet is widely perceived as 'a haven for pornographers, terrorists and hackers'. *The Guardian, 12 October 1995*

> Detective Superintendent Brian Drew of NCIS said: "Criminals are diversifying. They are using the tools that the Internet provides. Interception of these communications is very difficult."

> Mr Drew suggested the possible creation of new laws which would enable police to carry out monitoring and interception of communications. *The Guardian, 29 May 1997*

Aside from use of the Internet by terrorists and other criminals, there are also concerns that it creates a vulnerability which terrorists will exploit in order to cripple communications:

> The US government's greatest concern, however, is that terrorists or even hostile states could cripple communications networks that are vital to the running of the national infrastructure. Ironically, the Internet was developed to guarantee exactly that sort of infrastructure in the event of an atomic strike by the Soviet Union. Instead, it might now turn out to be the architect of disaster.
>
> ... Possible targets could be financial networks, including those of the main banks and the Wall Street trading floors, air traffic control computers, the power grids and the systems at the centre of national defence. *The Independent, 7 June 1996*

Yet this issue was tested very recently:

> The White House and the FBI announced a joint investigation last night into the biggest ever attack on the 13 computers that are the crucial basic components of the internet.
>
> For at least an hour from 9.45pm British time on Monday, the internet's 13 "root server" computers ... were deluged with massive amounts of extra data, creating bottlenecks that prevented legitimate data from reaching its destination.
>
> Seven of the servers were completely paralysed and two failed intermittently. ...
>
> ... Despite its scale, though, few internet users would have noticed this week's assault, partly because of its short duration and partly because the Internet's framework has the capacity to continue to function partially without the afflicted computers.
>
> ... backup versions of much of the relevant information is often already stored in "caches" at lower levels of the infrastructure, meaning that the root servers do not need to be consulted. *The Guardian, 24 October 2002*

Far from disaster, the Internet proved that its resilience is everything its architects had intended it would be. Concerns about the communications vulnerabilities created by the Internet and extent of damage which terrorists might be able to cause appear to be overstated.

Perhaps the most widely reported technology issue in recent years, aside from the Internet itself, is that of encryption. If the potential of Internet-based communications is to be realised, encryption is an essential tool for assuring security in communications, allowing verification of contracting parties (PKI, for example), safe passage of commercial information, protection of personal privacy and so forth. Yet one claim has overridden all of these positive benefits: that terrorists and other criminals might use encryption, thereby rendering their activities safe from the eyes of law enforcers.

> With encryption becoming ever cheaper, more powerful and more difficult to crack, a halt to progress may come from an unlikely source: our intelligence agencies. Correspondence between the British and US governments ... reveals concern about encryption at the highest levels.

> In May 1999, Janet Reno, then US Attorney General, wrote to Jack Straw, then Home Secretary, saying: 'I believe that the difficulties that encryption will pose for law enforcement are among the greatest challenges we will face in the coming years.' Straw replied: 'I fully share your concern at the threat posed by criminal use of encryption.'
>
> Since then, the 11 September attacks have added urgency to official eavesdropping, and new laws make it easier for law enforcement agencies to confiscate encryption codes. They are unlikely to countenance any technology that makes it more difficult to catch terrorists. *The Observer, 18 May 2003*

To curtail the use of encryption ignores two facts. First, the use of encryption brings enormous benefits to society, particularly in the spheres of commerce and personal privacy. Second, there are many ways to catch a terrorist, and it is unlikely that law enforcers would stumble on a hive of terrorist activity through wide-spectrum monitoring of unencrypted Internet communications without first having some alternative intelligence pointing them in a particular direction. Terrorists exist in real time and space, and this is where they will be caught. An encrypted email may hamper an investigation, but curtailing use of encryption for this reason alone seems to be a disproportionate response to a technology which has potential benefits to the wider society. In any event, it may be a moot point:

> Much of the commentary has focused on the use of encryption technologies, but this is a red herring. There has been no reported evidence that the terrorists actually used encryption. Moreover, the use of encryption is still relatively rare. Fewer than 1% of the billions of emails sent around the world each day are encrypted. *The Guardian, 22 November 2001*

1.3 Target of attack

There is disproportionate concern expressed in the UK national press that cyberterrorists will attack government and CNI systems.

> ... Possible targets could be financial networks, including those of the main banks and the Wall Street trading floors, air traffic control computers, the power grids and the systems at the centre of national defence. *The Independent, 7 June 1996*
>
> Britain faces a growing threat of an electronic attack by terrorists linked to al-Qaida that could paralyse key public services, including electricity and water supplies, the government's adviser on computer security has told the Guardian.
>
> For terrorist groups like al-Qaida with limited resources, it would be "a very attractive method" of attack, that would cause "huge damage", said Stephen Cummings, director of the National Infrastructure Security Coordination Centre. *The Guardian, 12 August 2002*
>
> Cyber criminals and terrorists will win an "arms race" against law agencies unless action is taken, a government-commissioned report said yesterday. *The Guardian, 12 June 2004*

Similar arguments are reported to hold sway in the US:

> Last week, another role was quietly created.
>
> Richard Clarke was appointed President Bush's principal adviser on cyberspace security.

> Fearing hacker attacks on, for example, the world's money transfer systems, stock markets, or nuclear facility control centres, the US rightly regards virtual terrorism as a real threat and something that is relatively easy for bad guys to do. *Mail on Sunday, 14 October 2001*

Evidence from hackers and the information security industry suggests that, far from being "easy to do" a virtual takeover of, for example, a nuclear facility would be immensely more difficult than organising a well-sited explosive device. However, the newly appointed Presidential advisor on cyberspace security set about proving his point, although it is not clear how much information the hackers might have been given in advance.

> Behind the scenes, Clarke was slowly trying to stiffen the administration's spine - and hunting for new options. To demonstrate America's vulnerability, he organised a group of government-paid hackers to break into the Pentagon's most secure computer systems in 1998. They gained control of the nation's military command centre systems - the very ones to be used to defend America during an attack. It took only three days and a batch of off-the-shelf PCs. *Sunday Times, 20 January 2002*

Firstly, it has been argued above that there is no solid evidence that terrorists are planning attacks on government or the CNI, and it is certain that no such attack has occurred to date.

> Despite fears that terrorists would use the internet to cripple infrastructure such as power grids, financial systems and telecommunications networks, the research showed that there had not been a single case of cyber terrorism in the six months to December 31. *The Times, 3 February 2003*

Secondly, ordinary hackers should, surely, be of more concern since their credentials in being able to penetrate government and military systems are proven – witness, for example, Gary McKinnon's hacks into US defence systems in the months around 9/11. Thirdly, there is no evidence to suggest that government and the CNI hold privileged status as targets, since the overwhelming majority of deliberate hacks and random security breaches occur in the private sector.

> Cyberterrorising is more often than not directed at opposing groups, rather than governments. In the Israeli-Palestinian battle, criminal hackers, or "crackers", on both sides are constantly attacking one another's web sites. A Pakistani cracker once stole the credit card numbers of members of a pro-Israel lobbying group and posted them online.

Private sector security breaches are a considerably bigger problem and the potential consequences are, arguably, no less significant.

1.4 Outcome of attack

Perhaps the most flamboyant of claims about cyberterrorism are reserved for the issue of what damage cyberterrorists might be able to cause. Death, nuclear explosions, plane

crashes, flood from breached dams, electricity outages, drug overdoses, all these have been heralded as possible outcomes of a cyberterrorist attack.

> My greatest concern is that hackers, terrorist organisations, or other nations might use information warfare techniques as part of a co-ordinated attack designed to seriously disrupt infrastructures such as electric power distribution, air traffic control, or financial sectors; international commerce; and deployed military forces in time of peace or war. *The Observer, 7 July 1996*
>
> President Bill Clinton will announce plans this week to build ramparts against a new and invisible enemy threatening to spread more chaos in America than any conventional terrorist attack.
>
> He will unveil defence measures unprecedented in the history of human conflict to protect America from the potentially devastating peril posed by cyber warfare, in which computer systems controlling airports, hospitals, traffic lights, banks and even nuclear weapons could be destroyed, creating havoc. *Sunday Times, 17 May 1998*
>
> The al-Qaida terrorist network has been making preparations for potentially devastating attacks on America by hacking into computer networks to look for ways to disrupt electricity and telephone systems, dams and nuclear power stations, it was claimed yesterday.
>
> Government officials said the terrorist group appeared to be far more sophisticated than initially thought in its use of the internet as a weapon to disrupt America's web-based economy and cause potentially catastrophic physical damage by opening dam floodgates or blacking out air traffic control systems. *The Guardian, 28 June 2002*

These examples are all important, because they deliberately paint a very vivid picture, one in which the very fabric of our society begins to unravel. These claims are based on the idea that our vulnerability rests on our dependence on computer systems, and claims-makers play on these keenly-felt vulnerabilities by spinning disaster scenarios for public consumption:

> A US defence department report earlier this year described how an information warfare attack might unfold. It starts with an unexplained power blackout in a large city. Telephone systems across the country become paralysed. Freight and passenger trains collide. Civilian air traffic control systems go haywire. Malfunctioning pipeline-flow control mechanisms trigger oil refinery blasts.
>
> As alarm spreads, "logic bombs" disable the financial system, disrupting money transfers and causing stocks to plunge on world exchanges. Automatic teller machines randomly credit or debit customers' accounts. Sensitive weapons systems malfunction.
>
> "(An) information war has no front line," says the study. "Potential battlefields are anywhere." *Sunday Times, 29 November 1998*

Individually and as a society, we are, the argument goes, at risk whoever and wherever we are: physical boundaries and barriers mean no thing any more. No-one is safe. But these disaster scenarios cross the boundary from worst-case scenario into the realms of science fiction. The evidence of some hackers and information security experts is, as explained above, that any one of these attacks would be no mean feat in itself, probably requiring insider assistance. Moreover, these scenarios wilfully ignore the failsafe systems which are undoubtedly built into the CNI.

> And even should a cyberterrorist attack prevail and shut down the power grid or disrupt the emergency response system, "these sorts of outages and problems tend to happen by accident already, so we have workarounds for them", Schneier argues. "What we don't have workarounds for are people flying planes into buildings or blowing up embassies." *The Guardian, 24 April 2003*

Bruce Schneier, chief technical officer of Counterpane Internet Security, makes the point perfectly. Estimations of the degree of damage tend, in any event, to be overblown. Even a successful attack on the CNI is unlikely to produce damage on the scale claimed, and this has been seen elsewhere with other technology-related concerns:

> Despite many people's initial concerns about internet banking, the losses from hacking into people's accounts have so far been negligible. Not that there has been a lack of attempts. Using a technique known as phishing, described by the US Federal Bureau of Investigation as "the hottest and most troubling new scam of the internet", fraudsters send out bogus e-mails asking customers to reveal their account details. Most major banks have already been targeted, but the amateurish nature of the e-mails has limited their success. *The Times, 24 January 2004*

1.5 Reaction to attack

There is scant evidence suggesting that cyberterrorism is likely in the short- to medium-term. There are far more pressing issues which warrant at least as much, if not more, attention than cyberterrorism but concern about the latter continues to escalate regardless. Claims about possible sources, method, target and outcome of cyberterrorist attacks are often wide of the mark and, on any common sense analysis, the concern these claims generate is disproportionate to the probability of harm or its likely scale. Cyberterrorism is, however, a *future* threat which is by definition unquantifiable and it is nowhere argued in this study that cyberterrorism will never happen. It follows that measures implemented now to guard against cyberterrorism in the future are not disproportionate in principle. Nor, in fairness, are they usually disproportionate in practice insofar as they are aimed squarely at *terrorist* activity. There are two major and related problems arising out of the formalised social response to cyberterrorism as enshrined in UK legislation and policy. First, measures which are ostensibly aimed at terrorist activity can in practice be used against ordinary criminals, bringing Draconian measures within the grasp of enforcers of the ordinary criminal law. Second, legislation pertinent to criminal law is promoted by reference to arguments about terrorism, thus distracting legislators and the public from debates about the way in which legislation is really intended to be applied and whether new law is proportionate or even necessary.

(a) Measures directed against terrorism

The prevention and prosecution of terrorism is always a politically and socially vexed question, raising as it does the spectre of unfettered power for the executive with limited

safeguards, transparency and accountability. Certainly, the terrible nature of the threat warrants a response beyond the ordinary criminal law, but the question of what response is legitimate and what goes too far is controversial. Recent developments in the law on terrorism, such as the row over detention without trial, demonstrate that feelings run high, an issue compounded by the contemporary climate of distrust of politicians:

> As Lord Nicholls said in his judgment: "Indefinite imprisonment without charge or trial is anathema in any country that observes the rule of law." Ian McDonald QC, who resigned as an advocate for the detainees, talked of "an odious blot on our legal landscape" that offended principles going back to Magna Carta.
>
> What we have at present is the worst of all worlds. The evil of entrusting our liberty to politicians is compounded by a lack of independent safeguards or transparency. *Sunday Times, 30 January 2005*

Central to the issue of proportionality of response to terrorism is its definition. Even the most extreme counter-terrorist measures, if applied to only the most extreme and deadly forms of terrorism, are readily justifiable. However, the wider the definition of terrorism, the more it encompasses activities which are not quite so serious, nor so deadly, and the more extreme responses become much harder to justify, particularly when they start to infringe the civil liberties of those not themselves committing terrorist acts. This extract illustrates the problem:

> The war on terror is already proving a headache for environmentalists, taking them into murky legal territory. "It's a ludicrous extension of the word terrorist," says Steven Best, a professor of philosophy at the University of Texas at El Paso, who has written about the animal rights movement. "It drains it of any meaning."
>
> In the US, terrorism is usually depicted as politically-motivated violence towards people, but if terrorism is expanded to attacks on property, argues Best, then are corporations who destroy rainforests not also terrorists?
>
> "The semantics of this is very important," he says. "In order to apply anti-terror laws, you have to first define a group as terrorists. Once you have accomplished that, you can override constitutional protections." *The Guardian, 2 March 2005*

The beginnings of this dispute in its recent incarnation are found in the debates on what is now the Terrorism Act 2000. There were grave concerns about animal rights and environmental activism falling within the definition of terrorism but far more important for these purposes were the proposals to bring computer hacking within the definition of terrorism.

> Animal rights extremists and religious cults face bans under proposals to strengthen anti-terrorist laws. The Government also plans to adopt the FBI's definition of terrorism as being violent acts carried out by groups such as militant computer hackers and some anti-abortionists. ...
>
> ... "We propose to frame the new definition so that it is flexible enough to cover any terrorist threats which might develop in future, whether due to new causes or ideals or to terrorist use of technology." *The Times, 18 December 1998*

> Peers did, however, agree various government amendments aimed at extending the anti-terrorism legislation, including action to counter cyber-terrorism.
>
> The Lords voted to extend the definition of terrorism to include the use or threat of action "designed seriously to interfere with or seriously to disrupt an electronic system".
>
> Such action would be covered under the bill if it was done for political, religious or ideological purposes and if it aimed to influence government or intimidate the public. *The Guardian, 21 June 2000*

The Act now defines cyberterrorism in Section 1, the relevant parts being as follows: use or threat of an action designed seriously to interfere with or seriously to disrupt an electronic system in order to influence the government or to intimidate the public for the purpose of advancing a political, religious or ideological cause. This is a very wide definition of terrorism which does not require any threat of personal injury, merely the threat of electronic interference or harm and, on this basis, the full might of the counter-terrorism regime comes into play. The government justified this approach as:

> ... covering actions which might not be violent in themselves but which can, in a modern society, have a devastating impact. These could include disrupting key computer systems or interfering with the supply of water or power where life, health or safety may be put at risk'. *The Guardian, 3 December 1999*

However, there is no such qualification in the Act. Hacking can be a terrorist offence without any risk to life, health or safety, as long as it is done to influence the government or intimidate the public in order to advance a political, religious or ideological cause. A cyberterrorist attack resulting in malfunctioning of an air traffic control system whether or not anyone actually dies should be, and is, caught by this definition of cyberterrorism. That is the kind of future threat which is properly dealt with in the anti-terrorist legislative regime. But the Act does not stop there. On its face, it also defines as terrorist those Palestinian teenage hackers who deface the websites of Israeli organisations with pro-Palestinian and anti-Israeli slogans. The definition of terrorism is the gatekeeper of the state arsenal. If the definition is too wide, the state has access to that arsenal too readily. Such is the case here and there is clearly scope for the full spectrum of anti-terrorist measures to be wielded against hackers with a criminal, rather than terrorist, intent.

Although this over-wide definition of cyberterrorism is now on the statute books, there is still scope for limiting the extent to which emergency powers can be used against hackers through the use of concepts such as 'proportionality' of response. The Civil Contingencies Act 2004, which provides for emergency powers in relation to terrorism and other civil emergencies, nods in this direction with its requirement that emergency powers be proportionate to the nature and scale of the threat.

> Remember, emergency powers extended to governments under such acts are extensive. They include the right to confiscate, requisition or destroy private property; require people to evacuate specific areas; bar public access to particular sites; over-ride existing laws; and ban public gatherings or entire organisations. The original definition in the draft bill would have allowed unrestricted action on computer hackers and political protest on a wide range of issues. ...
>
> ... Six months on ... a new bill emerged. It is not yet perfect, but both Liberty and Justice, the two leading civil liberty groups, paid tribute yesterday to the changes which ministers had conceded. They include a tighter definition of emergency and new safeguards requiring emergency powers to be proportional to a perceived threat. *The Guardian, 8 January 2004*

Nevertheless, the definitions are still wide and these emergency powers could, in theory, be deployed in relation to what would normally be considered criminal acts which do not threaten life or limb.

Apart from these very wide definitions of terrorism, the idea of creating a government department to monitor the threat from cyberterrorism and related threats, to advise the government and to inform the public is beyond reproach. President Clinton did it in the US:

> Clinton will announce the creation of two government organisations to concentrate on monitoring the cyber threat and informing the public of the danger. He will also appoint a "terrorism tsar" to co-ordinate efforts to prepare for cyber warfare. *Sunday Times,17 May 1998*

The UK has similarly founded NISCC:

> ... in January last year Jack Straw, the Home Secretary, announced a "series of measures to minimise the risk of electronic attacks" including the setting up of a National Infrastructure Security Co-ordination Centre to alert key industries such as telecommunications, water and electricity. *The Times, 6 May 2000*
>
> A shadowy government organisation set up to protect Britain's infrastructure from "cyber attack" is investigating the love bug virus, as well as at least two attacks on government computers that have been linked to foreign powers.
>
> The havoc spread across the globe by the world's fastest-moving computer virus has brought to light the role of the National Infrastructure Security Coordination Centre (NISCC), a front for MI5 and GCHQ, the government listening centre. *Sunday Times, 7 May 2000*

NISCC did not remain 'shadowy' for long and now has a good reputation for the work that it does, particularly for its rôle in informing the public and information sharing programmes such as the WARP initiative outlined in Chapter 2. Perhaps the allocated resources are disproportionate to the scale of the threat of cyberterrorism, perhaps they are not, but there can be little harm per se in an organisation dedicated to threat assessment and advising the public. The problem comes later, when these new organisations are looking to justify or increase their remit or resources. As detailed above, Clinton's new terrorism tsar embarked on a hacking exercise to 'prove' the

extent of the threat to the US CNI. NISCC has also made some rather alarmist claims about the potential consequences of cyber-attack.

> Terrorist groups may try to infiltrate the computer systems of some of Britain's biggest companies, government departments and emergency services if a war is launched against Iraq, the Home Office has cautioned.
>
> Stephen Cummings, director of the National Infrastructure Security Coordination Centre (NISCC), said key IT systems were under threat of cyber attack by Islamic extremists.
>
> He said: "There will be groups attacking US Government and defence websites and similar groups carrying out activity against the websites of any country involved in military action."

This was an unequivocal prediction of cyber-attacks carried out by terrorists which never materialised. There was no evidence of increased hacker activity over the period of the second Gulf War, and none from terrorist sources (Chapter 6, Section 2.2 (c)). Nevertheless, even if the claims were overblown, the advice was sensible and outlined what organisations should be doing routinely to safeguard information security against hackers and terrorists alike:

> Mr Cummings urged businesses to step up security ahead of a possible war in the Gulf. He gave warning that terrorist groups might try to infiltrate activists into the IT departments of leading firms. ... Last year NISCC warned companies, including BT, Lloyds TSB and BAA, to beef up their IT security. *The Times, 20 February 2003*

Rather confusingly, there are a number of new agencies dealing with information security, including the former Office of the e-Envoy, the NISCC, the e-Government Unit in the Cabinet Office, the DTI's Information Security Policy Team and the Central Sponsor for Information Assurance. All seem to have some measure of responsibility for combating cyberterrorism, although the strategy is not yet entirely clear.

> The language is reserved, the discussions kept within a close circle of specialists, but security experts say the government is taking the threat seriously. In the United States, repeated warnings of an "electronic Pearl Harbor" from terrorism and technology experts have given the subject more public prominence. The White House is due to release a national strategy to secure cyberspace within the next few weeks. The UK's parallel effort, the "national information assurance plan", was revealed last May but is "still in its early stages", a spokesman for the e-envoy's office admitted. *The Guardian, 20 February 2003*
>
> ... the Government ha[s] embarked on a four-pronged strategy which involve[s] preventing attacks, protecting civilians, pursuing terrorists and preparing for the aftermath of an attack. *The Times, 23 March 2004*

This outline strategy seems fine as far as it goes, but suspicions have been raised about the lack of detail fleshing it out. This has led to claims that not enough is being done to protect society from the menace of cyberterrorism.

> But the Tory Shadow Minister for Economic Affairs, Michael Fabricant, who believes Britain is a 'prime target' for cyberterrorism, says the UK government does not take the threat seriously enough and is 'inviting trouble'. ...
>
> ... a Home Office spokesman admits: 'The US has put more money into this issue but this reflects the greater dependence that the US has on interconnected systems. It is for companies to take responsibility for IT protection and security issues themselves.' *The Observer, 6 June 2004*
>
> I [Toby Harris, Labour Peer] have sought through parliamentary questions clarity as to what measures are in place to protect against such attacks. The responses all referred to the pivotal role of the national infrastructure security coordination centre established in 1999. But the NISCC is only an advisory body and each element of the critical national infrastructure is responsible for its own defence - the NISCC does not even know how many computer systems comprise the UK's critical national infrastructure.
>
> In practice, no governmental organisation has operational responsibility for managing defence against systematic cyber-attack. MI5 is right to warn of such an attack. What is surprising is the degree of complacency about addressing the threat. *The Guardian, 17 November 2004*

It is interesting and, perhaps, telling that the UK government has placed relatively little emphasis on centralised administration of the national response to cyberterrorism when it has been so vigorous in promoting the problem in the first place and so proactive in establishing targeted legislation and corresponding powers for law enforcers. There are other anomalies, particularly the apparent lack of police resources, both in terms of technology and technological expertise, despite the statutory powers granted to them.

> How are Blunkett's boys in blue equipped for the fight?
>
> Hum, said my honest informant. We're almost ground zero. He was only allowed to send emails himself 18 months ago. He only got on the net in the office six months back. The five managers in the unit he works for have had to scrabble through other budgets, raising the £100 a head they need to log on. The rest of the department is still on the outside, sucking its collective thumb. The computers inside HQ don't interface with each other, let alone those of other forces. Force recruiters don't ask whether the new men and women coming in have IT skills. It's not a question on their screens - and if you do, by luck, happen to hire a slick operator, you lose him quick. Of course. The money outside is so much better. *The Guardian, 10 December 2001*

This lack of resources provides a check, however unintentional, on the wide-ranging powers available to the executive in relation to broadly-defined acts of terrorism.

> Why are those who advise the home secretary so keen to throw anything that "might" be relevant to a criminal inquiry into this stew? Well, they would be, wouldn't they? Never opt for a limited power when a generalised one is so much comfier. But the home secretary - like us - needs to ask who is licensing whom? Where are the dedicated squads of expert officers who know what to look for and how to look for it? What use is traffic data from AOL when you haven't got a terminal to call your own?
>
> ... The scope of what Mr Blunkett proposes has barely been recognised. The little matter of who will enforce it, and how, remains utterly mystic. (Yes, there is a small central hi-tech coordinating unit established this year - but it's still recruiting.) *The Guardian, 10 December 2001*

(b) Criminal measures promoted through terrorism

The analysis so far has focused on legislation directed towards terrorist acts which can, by means of wide definitions, be directed towards what would normally be considered ordinary criminal activities which would not usually be thought to merit the emergency powers applicable to terrorism. Another, connected, problem arises when ordinary criminal laws are justified with reference to arguments about terrorism.

As John Naughton of *The Observer* notes:

> This is where the dark side of the net comes in handy. If you are (say) a Home Secretary who seeks draconian powers to control the net, your best strategy is to scare the citizenry by exaggerating the risks from criminals and paedophiles to justify those powers. Since nobody knows the extent of criminal use of the network, you are unlikely to be challenged on empirical grounds. Blunt assertions from policemen and spooks are all you need. This was how the Regulation of Investigatory Powers Act was pushed through - giving MI5 access to every digital packet flowing through a British ISP's servers. *The Observer, 13 May 2001*

There are many methods of controlling the Internet, nearly all of which are applicable to criminal behaviour and most of which can and have been justified with claims that they will help in the fight against terrorism. The most controversial legislation in the UK in this respect has been the Regulation of Investigatory Powers Act 2000 which, despite its name, is usually thought of as granting powers to law enforcers rather than derogating from them.

> The Bill gives law enforcement agencies new powers to intercept e-mails and decode encrypted data. It requires Internet service providers (ISPs) to install "black box" traffic surveillance systems linked to an MI5 monitoring centre. Police and security services can then obtain a readout of all the websites a customer has visited and, with a warrant from the Home Secretary, inspect the contents of e-mails. These agencies can also demand encryption keys to coded information from individuals or companies, again with a ministerial warrant. *The Times, 12 June 2000*

> Police and MI5 access to bank statements, health records, private files in private places? That is only the beginning. The Home Office wants to sit astride the digital revolution. It wants internet service providers to keep (not junk) the records of every log on, every site visited, every email sent or received - and to produce them on demand. In parallel with that will go records of every mobile phone call you make, identifying (in the third generation) where you were and when to within a radius of 10 yards. *The Guardian, 10 December 2000*

These measures sparked huge controversy around the time the Bill was passed, most of which centred around the data retention provisions and those which allow requisition of keys to encrypted data. Most controversial of all, perhaps, was that these powers were accorded not only to the police and intelligence services, but to a wide array of other public bodies, including government departments and local authorities. The Act is worded to cover all sorts of criminal behaviour and yet ministers were keen to highlight only the most serious crimes and terrorism.

> The home secretary will insist that these provisions are to prevent drug barons, child-pornographers and terrorists from using technology to defeat the police. *Sunday Times, 5 March 2000*

But commentators noted the broad application of these powers and particularly the fact that they were not limited to terrorism:

> And all this isn't limited to combating terrorism itself. No, it affects anything "that might be relevant to a criminal inquiry". *The Guardian, 10 December 2000*
>
> On the face of it, these measures, aimed at combating terrorism, child pornography and organised crime on the Internet, may seem reasonable. But this Bill will do little to cow the online underworld; and it will, without doubt, infringe civil liberties and subject businesses to needless costs and uncertainties. ...
>
> ... No other country regulates the Internet in such draconian fashion. *The Times, 12 June 2000*

It was also noted that the powers may not even be effective against those committing the most serious crimes and terrorism.

> ...The inevitable price of fighting terrorism? Not quite. Hi-tech terrorists have their sophisticated "stealth techniques" that none of these powers can counter. Low-tech terrorists can merely log on once in an internet cafe or pinch a mobile phone then chuck it away. Such trawls, for the most part, will be routine business. ...
>
> ... No wonder the government's own information commissioner, Elizabeth France, is alarmed. No wonder she thinks this bit of the bill indefensibly broad, lacking all "proportionality", an affront to the European convention on human rights, a mockery of "data protection". *The Guardian, 10 December 2001*

That said, data retention is still an ongoing project for the UK government and the next stage was to seek EU coordination on data retention laws. Once again, these were justified as anti-terror measures, but they have much wider application to ordinary criminal matters.

> Charles Clarke will seek to win support from European Union countries tomorrow for contentious Europe-wide anti-terror laws on retaining personal data.
>
> The home secretary will call on the 25 member states to store telephone and internet records for at least 12 months as they review counter-terrorism work undertaken since the London bombings in July.
>
> At a meeting of EU justice ministers in Gateshead, Mr Clarke will stress the importance of the information to terrorism investigators. He will make his call for an agreement by next month amid industry claims that the measures could cost communications companies millions of euros each year and police warnings that they could be swamped with information. ...
>
> ... In a paper to be presented to ministers at the meeting, the UK says such data are the "golden thread" running through terrorism investigations. Some of the suspects in the attacks on Madrid last year were identified using telephone records. Hamdi Issac, a suspect in the failed attacks on London on July 21, was reportedly traced by his mobile telephone use.
>
> "I think we can make the case that our ability to retain data is a real and genuine plus in the war on organised crime and terrorism. We have done a lot of work on this and we

> also believe the issue of cost is not an issue," Mr Clarke said this week. *Financial Times, 7 September 2005*

Here again is the rather strange situation of government ministers pushing hard for new controls over electronic communications whilst the police warn that they cannot cope with this quantity of data. Communications service providers are also concerned about the considerable financial and administrative burdens placed on them. The Home Secretary weighs against these issues a few, very rare, cases in which communications data assisted in the investigation of a terrorist offence – investigations, not prevention. There is no suggestion that this was the only evidence available to the investigating authorities or that it was crucial to the investigation. Requiring the retention of data potentially affecting all communications service providers and users would appear to be a highly disproportionate response if the aim is merely to provide evidence which might be helpful in the few cases of terrorism which occur in Europe every decade. The response might be less disproportionate if the real intention is to use such data routinely in criminal investigations, assuming both that the police have the resources to make sense of such huge quantities of data and that society is content to allow it to be used in such a way. These are weighty assumptions. Although it is impossible to establish the truth, there are some who claim that there are strong reasons why the UK government and others need data retention legislation, even if these are not the reasons given:

> Simple Nomad is a senior security analyst for BindView Corporation and a founder of the Nomad Mobile Research Centre, an internationally known group of hackers. He is concerned about how governments are using the cyberterrorist pretext to "sniff" personal email and web traffic. ...
>
> ... In the name of cyberterrorism, there is more funding than ever going into the listening and data sniffing capability of governments." ...
>
> ... He says one of the biggest "sniffers" is the international Echelon project, set up by western governments to sniff the net, telephones, and almost everything digital to provide intelligence for the security services. Most of Echelon is large scale, to do with all telecommunications - which is why, he says, national governments have had to introduce such legislation as the UK's Regulation of Investigatory Powers Act to be able to monitor pure ISP internet traffic. *The Guardian, 5 December 2002*

Some corroboration for this view can be found in a European Parliament report which noted that US and UK intelligence services had used Echelon to filter both private and commercial communications.

> ... a European Parliament report this summer ... said the US and the UK had used a communications spying system called Echelon to "intercept, at the very least, private and commercial communications, and not military communications."
>
> Ironically, the report recommends that individuals and companies encrypt e-mails as a matter of course to protect themselves. *The Daily Telegraph, 21 September 2001*

Encryption has been feared by the US and UK governments alike since the mid-1990s. The UK government mooted a key escrow arrangement in the 1990s, but it was hugely unpopular and never became law. There are now provisions in the Regulation of Investigatory Powers Act 2000 which allow the authorities to compel the disclosure of encryption keys, but these provisions remain unpopular and are not yet in force.

A second, high-profile example of an instrument of civil and criminal control being justified as an anti-terrorist measure is the case of identity cards. This time, the police are in favour.

> Metropolitan Police Commissioner Sir John Stevens has no doubts. Warning that Britain is at its highest level of alert in its peacetime history, he described the introduction of compulsory identity cards as an absolutely essential tool in the war against terrorism. ...
>
> ... Home Secretary David Blunkett says an ID card scheme will tackle such serious issues as illegal working and immigration abuse as well as fraud, terrorism and organised crime. *Sunday Express, 16 November 2003*

However, it is far from proven that identity cards would be effective to prevent terrorism or crime more generally. There may, indeed, be unintended consequences, such as actually increasing the opportunities for crime and increasing security risks to individuals through the establishment of an identity database.

> The great myth about ID cards is that they make us safer.
>
> France has a national ID system that made no difference to the terrorist bombing of its Metro system.
>
> Turkey has ID cards without making the slightest impact on rampant crime.
>
> And it is worth remembering that those who hijacked the planes in the US all had full sets of ID documents that took them into the country and through airport controls. *Morning Star, 2 October 2001*
>
> Most damning for the Government is the fact that the study does not believe the ID system as proposed will fulfil any of its intended functions such as curbing identity fraud or countering terrorism. If anything, the existence of such a large database and the assumption that the system is foolproof, when it is likely to give false readings, will make it vulnerable to hacking and fraud.
>
> Professor Ian Angell, of the LSE's IT department, said the scheme was a "one-stop shop for fraudsters". "It is a dog's dinner. I do not believe it is going to work." *The Daily Telegraph, 28 June 2005*

It has been argued by many that the invasion of privacy, the financial cost to individuals and the state and the risks inherent in setting up an identity databases are not proportionate to the intended benefits of fighting terrorism and crime which are, in any event, unproven. These arguments of proportionality have taken place in protracted debates at the highest level. It is not the purpose of this study to state a definitive opinion on that issue. It is necessary to note that the use of identity cards will, in the

main, be restricted to civilian and ordinary criminal matters and the extent to which the cards have been touted as a panacea for terrorism of any kind is clearly disproportionate to the likely extent of their use for this purpose. Moreover, focussing on the headline issues and ignoring the everyday mechanics of operating such schemes may lead to a failure to consider adequately the potential for unintended consequences. An identity database raises the possibility that this will become a focus for hackers, both criminal and terrorist, effectively adding a future threat to the long list of threats the scheme was meant to address in the first place.

> The case against identity cards rests on proportionality. The invasion of privacy and cost are disproportionate to the benefits. ... Any serious crook or terrorist will undoubtedly find a way to avoid detection. ... And, of course, the better the system, the more incentive for the wrongdoer to crack it. And we can already see internet hacking getting increasingly sophisticated. *The Times, 31 May 2005*
>
> ... the Government's ID card plans [are] an "insane scheme to give £10 billion of taxpayers' money to the IT industry". ... "It's not so much the fact that they won't work as advertised, or even the cost. It's the database behind it, which will provide a big target for hacking." Improbulus quoted a child of ten: "They can fake passports, so why can't terrorists copy ID cards?" *The Times, 2 July 2005*
>
> Peers also warned that it would not be possible to protect the cards from hackers, making them a security risk rather than the answer to the threat of terrorism. *The Mirror, 16 November 2005*
>
> In truth, the government is establishing a mouth-watering target for fraudsters and terrorists. Anyone who hacks into the national identity register can make a fortune or reduce Britain to chaos. *Sunday Times, 3 July 2005*

There are many other such examples, where proposed laws or policies are either unlikely to address the problem they are aimed at or are more likely to produce unintended consequences, or both. In the mid-1990s, German authorities tried to prevent German citizens from accessing Radikal, a left-wing magazine, illegal in Germany, the electronic version of which was available to German citizens from a Dutch web host via German ISPs. The German ISPs tried to block German users from accessing the Dutch website. The Dutch web host appealed to censorship campaigners:

> Net activists responded by putting up mirrors of Radikal - at last count there were 47 worldwide. ...
>
> ... As for the German government, their problems seem to be just starting. Thanks to some hamfisted action, a little-known magazine they didn't like is now all over the Net. 'The big question is, will they now block the 47 Radikal mirror sites,' ... 'But if they do, it could create an international scandal, because there are lots of US sites involved.' *The Guardian, 26 September 1996*

Following the same logic, the police in the UK are similarly risking escalation of the problem they are seeking to address if they are granted the powers they seek to attack various websites connected to terrorism:

> The Association of Chief Police Officers (Acpo) recently called for "powers to attack identified websites" as one of 31 new measures to tackle terrorism. ...
>
> But will it work? Already, "if (a website is) hosted in the UK, it should be relatively straightforward to get the host to remove the content," says Struan Robertson, senior associate at law firm Pinsent Masons. This is because internet service providers usually remove sites when asked to do so by the police. Robertson adds that if legal pressure is required, the Terrorism Act of 2000 makes it an offence to provide or receive instructions in the making or use of explosives.
>
> However, many explosive-making sites use domain names registered to owners in the US (although they could also be hosted elsewhere). The US has a law prohibiting online instructions for bomb-making, but Richard Clayton, treasurer of the Foundation for Information Policy Research, says the country is a popular location for such sites because of the cultural and constitutional support for freedom of speech. "There's a strong lobby here, so these sites will continue to exist whether the British police want them to or not," he says. *The Guardian, 4 August 2005*

So, if the objectionable site is hosted in the UK, the police do not need a new law to take it down. If it is hosted in the US, constitutional commitments to freedom of speech make it unlikely that any new law in the UK would be effective. If the site is hosted elsewhere, the UK police may or may not achieve its removal, but in any event risk the site being mirrored elsewhere, perhaps many times over, raising its profile in the process.

Likewise, routine use of the data mining technology Echelon by the US and UK intelligence agencies risks incentivising users towards greater use of encryption technologies, thereby rendering communications impenetrable. Introduction of biometrics into identity tokens may also raise more problems than it solves:

> The Passport Service's six-month trial of biometric passports will be used to justify ID cards as a solution to terrorism or identity theft. But concerns will grow about the high number of false positives given by facial-mapping software, and those seeking to disguise their identity will find ways of falsely recording their details on the underlying database. *The Times, 6 January 2004*

Previous examples show how a particular response to a problem may actually exacerbate it. This last example is especially worrying, however, and sums up many of the problems discussed in this section because it raises the possibility that totally innocent people might be identified and treated as terrorists or criminals. The chances of preventing a terrorist attack through biometric identity cards alone is negligible. On the other hand, they significantly increase the chances of harm or disruption to innocent individuals who are mis-identified. By focussing on the anti-terrorism argument, those who want such measures introduced – identity cards, extensions to emergency anti-terrorism powers, data retention – are able to brush to one side the arguments about proportionality.

> The thinking behind it was laid bare, even celebrated, in Tony Blair's speech at the Labour conference, where he dismissed concern for freedom as 'libertarian nonsense'. But perhaps the most alarming illustration of Labour's tin ear for liberty came this week, with the publication of Jack Straw's anti-terrorism bill. It is a dangerous document, violating some basic, precious fundamentals of human freedom. *The Guardian, 4 December 1999*

The public is asked to trust its leaders, not to ask awkward questions. If the leaders are taking more power than they strictly need, the public should be reassured that they will not use those powers unless they are really necessary and then only to fight terrorism.

> So the secrecy is justified. The government knows more than we do. What we don't know is for our own good. Leave it to the administration. Trust Daddy. Close to half of the voting-age population in America appears to subscribe to that view, while the other half fears that democracy itself is being fatally undermined by the administration's unseemly eagerness to exploit every available political possibility of this war (which isn't quite a war) on terror (which, as an abstract noun, is unlike any enemy ever caught in the sights of a sniper's rifle). *Independent on Sunday, 11 January 2004*

Summary

The debate on cyberterrorism is part of a wider debate on terrorism, organised crime, national security and personal freedom. When politicians and other claims-makers amplify the risks from cyberterrorism – whether in terms of the existence of cyberterrorists, their methods, targets and the potential outcomes of attacks – they are contributing to the pressure which is being exerted more generally for increased security through new measures of social control at the expense of personal freedoms. This is the broader issue. There is a narrower issue: that of control of the Internet and the communications it facilitates. Disproportionality is found in the amplification of the negative aspects of the Internet and other technologies and attenuation of their corresponding and immeasurably greater benefits.

When the individual legislative measures relating specifically to cyberterrorism are examined, there is little against which a serious objection could be made, if only the actions against which they are targeted have sufficient terrorist motive and are sufficiently destructive to qualify as terrorism, rather than hacking or any other crime. This is not the case, and over-wide definitions of terrorism are beginning to open up the possibility for the most severe anti-terrorist measures to be applied against standard criminal activities. In addition, ordinary criminal laws are often justified by appealing to the fight against terrorism, so that genuine concerns about their wide application, their proportionality, their effectiveness and their effects on human rights and civil liberties are side-stepped and passed by.

These important issues will be discussed further in the following chapter.

2. VOLATILITY

Volatility is the last of the five elements of a moral panic outlined by Goode and Ben-Yehuda (1994). The essence of a moral panic is that it rises up quickly; concern reaches a high level, perhaps even fever pitch; consensus is established as to what the problem is and who is responsible; hostility is displayed towards those identified as responsible; the perceptions of the situation and the means of its resolution are wholly disproportionate to an objective assessment of the level of threat; finally, the scare dies down, often as quickly as it rose.

However, as Critcher points out (Critcher 2003: 151), volatility is one of the least useful attributes of a moral panic and is extremely difficult to test. This is because it is not possible to place temporal boundaries around the concept of volatility: a panic may last a few weeks or a couple of years; there may be a drawn-out period of concern punctuated by highly volatile episodes; the panic may even be serial in nature, each one building on the last. The panic about cyberterrorism did not rise up quickly and it has not died down, so the findings on volatility are quite simple: the concern about cyberterrorism is not volatile in the long term. As Figures 1-4 in Chapter 5 demonstrate, press coverage has risen steadily over the last 20 years. Reporting levels in the national press are high – it is certainly a hot topic – and there is no evidence of it tailing off. This is not the pattern of press reporting Goode and Ben-Yehuda expect from a full-blown moral panic: little or nothing one day, very high levels of coverage the next, continuing, possibly increasing for a period, then dying away just as quickly.

There were, however, points at which cyberterrorism received more coverage than usual. Figure 2 in Chapter 5 shows a peak in the second quarter of 2000 which was almost entirely due to a mini-panic caused by the 'I Love You' virus. The highest peak, in the fourth quarter of 2002, had no single cause, although widespread reports identifying Gary McKinnon as the UK hacker responsible for a number of US defence system intrusions over a two year period were by far the most numerous. This episode marked a period of high sensitisation to the issue of cyberterrorism. Another peak in the third quarter of 2005 was again partly attributable to the McKinnon saga and partly to high levels of concern about Government plans for ID cards and a related database. The narrative on this issue locates a paradox in which these measures are presented by the Government as part of the solution to terrorism but in themselves may make society more vulnerable to attack by hackers and terrorists if the database and related systems are not sufficiently secure.

Cyberterrorism appears to be an issue with staying-power, with generally increasing levels of concern being punctuated by periods of increased intensity. This despite the fact that no confirmed cyberterrorist attack has ever been reported. The reasons for this remarkable state of affairs will be discussed in the following chapter, which will concentrate on the social mechanisms at work.

SECTION III

THE FINISHING

CHAPTER 9

DISCUSSION AND CONCLUSIONS

1. RECAPPING THE ATTRIBUTIONAL MODEL

The chapters in Section II have set out in detail the findings of this study organised according to the attributional model of moral panic developed by Goode and Ben-Yehuda (1994) and elaborated by Critcher (2003). According to this model, all the boxes have been ticked for a moral panic in relation to cyberterrorism except one: volatility.

1.1 Concern

Concern about cyberterrorism has been expressed in the press, by politicians, police and security services, the information security industry and other experts, including academics. There is no particular evidence of public concern, but this is not strictly necessary for the constitution of a successful moral panic (Critcher 2003: 150).

1.2 Hostility

Three main objects of hostility have been identified in the discourse on cyberterrorism: hackers, terrorists and technology itself. When the three are blended together using the classic mechanisms of exaggeration, distortion, symbolisation and prediction (future threat scenario), the mythical cyberterrorist emerges, ready to be cast as a folk devil for the Information Age. Cyberterrorists are characterised unambiguously as the 'enemy', harmful and threatening to the values and interests of society, especially those of personal privacy and national security. There is a duality in the social anxiety relating to technology itself because it is both the cyberterrorist's weapon and target.

1.3 Consensus

The cyberterrorist narrative is not uncontested. Although the vast majority of press coverage of this issue is hostile and reinforces the message that cyberterrorism is either already present or an imminent danger, there are those who challenge this view. They propose an alternative position, that terrorists are not ready to turn to cyberterrorism and that conventional terrorism and cybercrime are activities which are both current and in need of a targeted solution. This receives some press coverage and some journalists even accept the view that cyberterrorism is a useful construct for a government

desperate to exert more control over the unruly domain of the Internet. Nevertheless, the messages of caution are largely attenuated in the press and the dominant view is undoubtedly that which considers cyberterrorism an immediate danger.

1.4 Disproportionality

All available evidence points to the fact that no terrorist group has ever successfully carried out a cyber-attack causing significant damage to persons, property or the economy, nor are they imminently likely to do so. Any claims that they have or concern that they are imminent exaggerate the scale of the problem and are, therefore, disproportionate. There is also copious evidence of distortion of the issues, for example the relabelling of hackers as 'cyberterrorists' and of cybercrime as 'cyberterrorism'; the various claims that al Qaeda is actively pursuing a cyberterrorist agenda; the construction of technology as inherently dangerous and even 'evil'. All of these claims and more divert public attention away from the real dangers from conventional hacking and cybercrime towards the mirage of cyberterrorism.

1.5 Volatility

Critcher recommends that the element of volatility be abandoned (Critcher 2003: 151). Nevertheless, a true moral panic has a beginning, middle and end. It is possible to locate the beginning of the discourse on cyberterrorism, although it is less evident when this discourse begins to resemble a panic. As for the end of this episode, that lies in the future as it appears to be ongoing. What can be identified are a series of peaks in concern generated by specific events, such as the development of a new technology or the identification of a particularly prevalent virus. This points to the conclusion that cyberterrorism is a persistent issue and a peak may occur at any moment, giving it the appearance of a serial panic. Concern about the issue, measured in column inches, is indisputably growing year on year and higher levels of concern probably lie in the future, generated by growing technological dependency and a corresponding sense of vulnerability.

1.6 Claims-makers

Critcher added this sixth attribute to the original list of five because claims-makers are fundamental to the constructionist perspective espoused by Goode and Ben-Yehuda (Critcher 2003: 151). The claims-makers in relation to cyberterrorism are quite clear: politicians, the information security industry and, to a lesser extent, police and security services and other 'experts'. The press also functions as a claims-maker in its own right. There are many different strategies for claims-making, but by far the most

important for all claims-makers is the future threat scenario. The claims made can be characterised as exploitation, using the mechanisms of deviance amplification and orchestrating social reactions to achieve either social control or economic advantage.

Accepting that the criterion of volatility, at least as it is narrowly conceived by Goode and Ben-Yehuda, should be discarded, all the ingredients for a moral panic about cyberterrorism according to the attributional model are present. Yet, intuitively, this does not seem sufficient. The bare bones of this model as applied to this case do not expose adequately the reasons why concern is expressed, the importance of the media, the processes involved in social control and historical context. In fact, this information is available in the preceding chapters, but only because the material was merely organised according to the attributional model and the analysis, as such, took a grounded approach so that no significant information which came to light during the content analysis was left out. This is why Cohen's processual model is required, with the addition of attention to the construction of moral boundaries and underlying discourses.

The processual model, as elaborated (Critcher 2003:151), is made up of a discussion of a series of elements: emergence, media inventory, moral entrepreneurs/claims-makers, experts, élite consensus and concern based on distortion, coping and resolution, fade away and legacy. Critcher notes the need to add two further dimensions to the existing processual model: discourse analysis and establishment of moral boundaries (Critcher 2003: 177). Definition of social problems usually involves a variety of competing discourses, but a hallmark of moral panic is the development of a closed, incontestable discourse, the genesis of which should be identified in a model of moral panic. Critcher does not prescribe how discourse analysis should be merged with the processual model, but it fits neatly within the existing processual framework and this is how it will be discussed below. Critcher further notes that moral panics result in an "expression of irreducible moral values", reaffirming the moral boundaries of society with deviants on the outside. This seems obvious, but should be made explicit in any account of a moral panic using the processual model. The remainder of this chapter will cut across the findings of this study using these tools to expose what is missing from the cyberterrorism story.

2. EMERGENCE

A moral panic does not emerge from nowhere: it has its roots in an existing discourse. Previous moral panics have been based on discourses of youth (Mods and Rockers),

childhood (paedophilia), and drugs (rave/ecstasy). The emergence of the cyberterrorist is rooted in two enduring meta-discourses relating to technology and terrorism. The fundamentals of the discourse on terrorism are relatively stable, despite changes in the nature and source of terrorism itself. Terrorists are unequivocally evil, irrational murderous and destructive, threatening the lives of innocent and unsuspecting individuals going about their daily business. They operate outwith the boundaries of society and are excluded from political debate. Exceptional legal regimes are constructed to allow law enforcers and security services special powers of investigation and detention and penalties on conviction for terrorist offences are severe. Terrorists are in some circumstances denied even the normal due process rights accorded to other criminals because their crimes are considered so heinous. The language of risk is habitually adopted by politicians, law enforcers, security services and the media, with phrases such as 'level of risk', 'terrorist threat' and 'vulnerability to security breaches' being common. There is very broad consensus on these issues and the underlying themes of good against evil are well-established, pervasive and largely uncontested.

The discourse on technology is less homogeneous, but there is a strong narrative referring to technological dependency bringing with it corresponding vulnerabilities. The public feels a collective insecurity inspired by awareness of its own ignorance of how the technology works and an inability to control it, combined with the anxiety that there are others, hackers, who have mastered the technology, can control it and are somehow all-powerful (Skibell 2002). When this insecurity is coupled with the spectre of terrorism, it is a powerful brew indeed. In common with terrorism, the language of risk is pervasive. The hacker has come to symbolise these perceptions of risk and has been seen as an adolescent challenger to the adult order, bent on destabilising adult-created, computer-dependent systems (Halbert 1997). The insecurities of the Information Age, including the perceived lawlessness of the Internet, are summed up in the hostility towards this modern folk devil.

The image of the computer hacker has evolved over time, from 'kid with precocious powers' in the early 1980s; through 'pathological addict with unlimited powers' in the mid-1980s; then, when computer use was widespread among ordinary people so that the addiction tag was no longer appropriate, hackers became criminal, a threat to commerce in an increasingly computer-dependent business community (Skibell 2002). Hackers remain 'criminal' to this day, although the perceived dangerousness of their criminality has increased. Throughout this time, however, there have always been those who claim

that most hackers are law-abiding citizens who exist to push the boundaries of what technology can do. Hackers themselves have challenged perceptions of criminality, but the challenge has been unsuccessful because they lack cohesion as a community and do not present a united front. Sympathetic journalists have also challenged the hacker myth from time to time. Nevertheless, these counter-claims are attenuated in the press and the dominant discourse characterises the hacker as criminal and now dangerous.

The latest evolution in the construction of the hacker is the attribution of terrorist qualities. Here the discourses of terrorism and technology intertwine and their common language of risk allows this to happen almost seamlessly. There is perceived to be a novel threat, the cyberterrorist, whose form is constructed on three fronts. First, the hacker is repackaged as a terrorist and ordinary cybercrime is relabelled as cyberterrorism. The stakes have been raised so that, whereas before the hacker challenged personal privacy and commercial interests, now he is a threat to national security. Second, the use of ICTs by terrorist groups, mostly for communication purposes, is characterised as cyberterrorism. Although the available evidence indicates that cyberterrorism in the sense used in this study does not yet exist, this has not prevented claims that it is a reality or that it is at least imminent. Vulnerable targets are perceived to include air traffic, trains, dams, electricity networks and nuclear weapons, in short, the CNI and military networks. Third, technology itself, particularly the Internet, is implicated in the new threat from cyberterrorism. The emergence of new technologies is often a flash point for fresh rounds of claims-making about how such technology might represent either a weapon or a vulnerable target.

The Internet and networks generally are crucial to an understanding of the emergence of the cyberterrorist. Whereas terrorism has historically been geographically bounded, the Internet appears to render insignificant national boundaries. Cyberterrorist attacks may originate in one country and have a target in another without the necessity for any physical proximity between attacker and target. Moreover, technology allows the attacker anonymity so that any attempts at forestalling an attack or locating the attacker after the event are inevitably compromised. In this way, security forces are impeded and the social order is threatened.

The media report on public anxiety about technological dependence and the influence of the Internet and related technologies on society. The extent to which these reports represent real feelings is unclear, but it is the invocation of public anxiety by the media rather than its reality which is important in a moral panic. Ordinary people must,

according to the media, use or rely on technology, yet they do not understand how it works, giving rise to mistrust. An extreme sense of vulnerability is created by the concept of interconnectedness: everyone is connected, everyone is vulnerable. Furthermore, there are well-rehearsed narratives about online criminality, not just hacking but also pornography, paedophilia and other sexual perversions, organised crime, drug-trafficking, espionage, theft, fraud and so on. The Internet is portrayed as both central to modern society and as a lawless domain, a hive of criminal activity. Thus, there are threats not only to social order, but also to moral order from deviant activities. The emergence of the cyberterrorist has come to symbolise all of this. By adding the element of terrorism to the existing concerns about technology and its effects on society, the problem becomes more obviously *moral*, a struggle between the good of social stability and the evil of terrorist attacks. More importantly, however, the threat is transformed from being an organisational information security issue to a national security issue. This is more fertile ground for claims-makers amongst the political élite wishing to exert greater social control over the use of technology and, more specifically, electronic communications.

3. MEDIA INVENTORY

3.1 Sensitisation

Deviance, crime, terrorism and certain popular types of technology are inherently newsworthy and are issues to which the media are habitually sensitised. However, the last two decades have witnessed a reinterpretation of some of these familiar events and objects. They are combined and reworked and, when viewed from different angles, the mundane and familiar becomes threatening and dangerous: cyberterrorism. Hackers, terrorists and the technology itself are variously the targets of blame and stories relating to one or more of these are now interpreted as being part of the cyberterrorist threat.

Reports about cyberterrorism started in the late 1980s and increased steadily year on year until late 1997 and the publication of a report of President Clinton's US Commission on Critical Infrastructure Protection (PCCIP 1997). The Commission made recommendations for the protection of the CNI from both physical and cyber-threats, but press reports focussed on claims about the real and growing threat from cyberterrorism, the calls for increased spending on computer security and the need for new government posts to coordinate the response. This apparently new vulnerability seemed to take the US and the rest of the world by surprise. Whereas hackers presented a nuisance, cyberterrorists appeared to present an imminent danger, threatening the very

underpinnings of society with attacks on the *critical* national infrastructure. For the first time, an internationally important, government-commissioned report identified cyberterrorism as a serious issue and called for an organised response. The profile of cyberterrorism had been raised to new heights and became firmly established as an issue about which 'something must be done'. Press coverage has continued to increase since then and at an accelerated rate.

Unusually for an otherwise high-profile issue, the broadcast media do not seem to be sensitised to the issues of cyberterrorism to any significant degree. This is a phenomenon which has been constructed almost exclusively by and through the press. Another interesting feature of media coverage is that cyberterrorism is an issue to which the upmarket press seem to be particularly sensitised and the downmarket press less so, although their interest has increased in recent years. The Times, The Guardian and The Independent, including the Sunday editions, feature as particularly important in the corpus. Nevertheless, the press generally do now seem to be sensitised to the issue of cyberterrorism as a social problem.

3.2 Stereotypes and folk devils

The findings of this study demonstrate how hacking, terrorism and technology are associated to produce something sinister for public consumption. The cyberterrorist is a stereotype, of course, but one constructed from other stereotypes. This is crucial to an understanding of the social reaction to cyberterrorism. Deviants become easier to demonise if they are dehumanised and the context of their actions is ignored. Stereotyping assists in this process because it distances deviants from the realm of the normal and acceptable and confirms moral boundaries, with the deviants firmly on the outside. The cyberterrorist, being a stereotype constructed from other stereotypes, seems to be doubly damned and the context of his deviance, cyberspace, enables even more distance to be placed between the cyberterrorist and reality.

> "Moral panics depend on the generation of diffuse normative concerns, while the successful creation of folk devils rests on their stereo-typical portrayal as atypical actors against a background that is overtypical." (Cohen 2002: 45)

This is a 'them and us' mentality and an example of the imperative in a moral panic to reduce complex social problems to simplicity, to which end the underscoring of dichotomous relationships – particularly good against evil – is useful. The differences in motivations between the hacker and the (cyber)terrorist have largely been suppressed. Their particular brands of deviance have been defined as being contrary to the stability of society, the personal safety of innocent citizens and national security. In this way,

hackers, terrorists and, later, cyberterrorists have been successfully constituted as folk devils, with ICTs at the heart of their activities.

Occasionally, a moral panic may fail because stereotypes are successfully challenged in the media, either by the putative folk devils themselves or by someone speaking up for them. In cases of a successful challenge, the object of attack will be highly visible, yet structurally strong. Terrorist groups are both of these things, yet they do not fight back, at least not in the usual way, since one goal of terrorist groups is to gain the very type of sensationalised, snowballing media coverage typical in a moral panic. A good, strong moral panic is just the thing terrorists crave. Although they may have the means to fight back, they do not have the motivation.

However, hackers are different. They may well object – and it is well known that many do – to being labelled terrorists and cast as folk devils. However, they are highly visible and, because of the fragmented nature of their community and their, and society's, inability to agree on the definition of a 'hacker', they are structurally weak. Clearly, they have the powerful mechanism of the Internet through which to publish their views, and many do. Nevertheless, new media cannot yet compete with the press in terms of stereotyping. Hackers have little influence with the press and have found it difficult to find a mouthpiece for their views. The stereotypes necessary for the successful construction of folk devils have, therefore, remained largely unchallenged.

The stereotypical hacker is an anarchic youth or criminal, challenging from cyberspace the social order to which ordinary people adhere. He is a young man or adolescent – this is an exclusively male stereotype – pale and spotty, dressed in black, solitary, anti-social, even sociopathic. The stereotype has him as a master of his medium, a technical wizard who has society at the mercy of his superior skills. The reality is that only a handful of hackers actually have the level of mastery attributed to them.

Terrorists are stereotyped as the embodiment of evil: mass murderers beyond reason, the very worst type of social outcast, spurned by society at the very highest levels. They are perceived as irrational and ruthless fanatics and, to the extent that their 'cause' is recognised at all, it is denounced as delusion and madness. They are excluded from society to such an extent that dialogue or negotiation with them is strictly prohibited, even when human lives are at stake. This stereotype is strong, enduring and uncontested in the mainstream media.

The Internet itself is stereotyped as a lawless place where criminals flourish and all manner of deviance, criminal tendency and perversions are catered for. It protects the guilty with anonymity and renders innocent citizens vulnerable. Children are sucked into the network, there to be groomed by paedophiles, transformed into hackers (script kiddies) or brainwashed in chatrooms. Adults fare little better, being exposed to pornography, risking identity fraud or theft of credit card details. The Internet is everywhere, dangerous and indomitable except by those with extraordinary skills and ill intentions: hackers and terrorists. This stereotype is not uncontested since the Internet and other ICTs bring undeniable benefits to individuals and society at large. Nevertheless, this narrative of hostility is strong in the press.

The stereotype of the cyberterrorist is a combination of all these things. He has extraordinary technical skills, borrowed from the hacker stereotype, and is capable of breaching even the tightest security. If ICTs are the cyberterrorist's tool, they are also his target. The message is that advanced societies are technology-dependent, which means that they fall apart if that technology is attacked. Air traffic controls, trains, dams, electricity networks and nuclear weapons are all vulnerable. Because he is a terrorist, the harm he seeks to cause is severe: disruption and destruction on a massive scale; paralysis of critical infrastructure; death and injury. He is far more dangerous that the hacker. The danger is often couched in terms of national security, but the implications are global. The Internet and other ICTs allow him to attack anonymously and at a distance from his target, giving him global reach yet sheltering him from reprisals.

There is, however, no strong visual image of the cyberterrorist. The stereotype really amounts to little more than a conceptual linking between terrorism and technology. For example it is claimed that al Qaeda relies heavily on technology to plan atrocities and will soon be branching out into cyberterrorism. However, the public image of Bin Laden and his followers are of men in desert dress, living in caves and holding guns. Bin Laden himself does not seek to promote an image of a man sitting at a computer, rather that of a warrior ready for conventional armed combat. The gun is the most immediate symbol of his rhetoric. A computer does not enhance this image.

Terrorists are more immediately associated in the public mind with bombs, guns, explosions, physical destruction, death and mutilation. All these things are far removed from the clinical intelligence required for a successful computer hack, remote from the physical world. Analysis of symbols, images and stereotypes associated with

cyberterrorism demonstrate that they are really those associated with computer hackers and the terrorism aspect is bolted on. Hackers are inextricably associated with the computers which serve as the tools of their trade. Terrorists are not. There exists a social vocabulary with which to discuss the risks posed by hackers and yet these risks have never been amplified to the status of a moral panic. Hackers are stigmatised and vilified, but not particularly feared. Sometimes they are even viewed in a positive light. This is why the visual image of the cyberterrorist is not particularly powerful or successful, although that conceptual link between terrorism and technology is.

3.3 Exaggeration/distortion, symbolisation and prediction

Exaggeration and distortion are essential features of a moral panic and contribute towards disproportionality in both perception of and reaction to the problem. In relation to cyberterrorism, there is gross exaggeration of the seriousness of the problem; the critical nature of the supposed targets; the extent to which society is really computer-dependent; the amount of damage a cyber-attack is capable of causing; and the skills possessed by would-be attackers. Distortion is equally important. Terrorist motives are imputed to hackers; the gravity of likely outcomes of a cyberterrorist attack is placed on a par with that of conventional terrorist attacks using bombs; it is claimed that terrorists are pursuing the cyberterrorist agenda with just as much vigour as their bombing campaigns. The language used is alarmist and sensational, deliberately highlighting the vaguely-possible, nightmare scenario and suppressing the highly-likely, mundane outcome or non-event.

Two very particular manifestations of exaggeration and distortion can be found in the processes of symbolisation and prediction. The socio-cultural effects of technology and global terrorism are two of the biggest current sources of social anxiety. When combined, they construct the terrifying prospect of a threat to the very fabric of society. The fear is that society is dependent on technology which, in turn, renders society vulnerable to those with absolute mastery of that technology who may use it to their own evil ends. The stereotypical cyberterrorist has come to symbolise this fear.

Other symbols can be identified, some of them stereotypes, others not. The stereotypical hacker is symbolic of electronic delinquency. The negative stereotype of the Internet – contrasting with the positive views which also exist – is symbolic of lawlessness, disorder and the negative aspects of globalisation. The much-used phrase 'electronic Pearl Harbor' is symbolic of catastrophic attack in the homeland (here the US) and underlines the new uncertainties generated by the increasing tendency of

electronic networks to render geographical boundaries insignificant. It is often reported that geographical boundaries no longer guarantee protection against criminal and terrorist attack. 9/11 has become symbolic of all the issues related to President Bush's War on Terror. Perhaps the most powerful symbol for decades, in the aftermath of the atrocity mere reference to 9/11 was sufficient to summarise a whole raft of justifications for governments to engage in offensive action abroad and repressive legislative regimes at home. In one date was encapsulated the national security agenda. Another date, Y2K, became a symbol of the inherent fragility and untrustworthiness of computers. Microsoft, at once a global business and a dominant retail product, is a symbol both of Western hegemony and of Western vulnerability caused by dependence on specific technologies. Claims that UK nuclear submarines were to be run on the notoriously insecure Windows 2000 platform were sufficient to trigger outrage: "The Government was accused last night of leaving Britain's nuclear arsenal wide open to terrorist computer hackers" (Sunday Express, 24 October 2004).

These symbols are powerful and are combined in myriad ways to convey the discourse of technology, terrorism and danger. Yet, this is not an accurate reflection of reality. So far as we know, and with the usual caveats about the classified nature of much information about terrorism, cyberterrorists do not yet exist. Their appearance in the press is almost entirely attributable to another distortion, a net-widening process such that previously unconnected activities, hacking and terrorism, become characterised as belonging to this particular class of deviance, cyberterrorism, by a process of re-evaluation and redefinition. Hacking, cybercrime and terrorist use of ICTs are relabelled as cyberterrorism. The presence of the cyberterrorist seems established, but it is a mirage. Net-widening through relabelling has resulted in exaggeration of the size, even existence, of the problem of cyberterrorism and a distorted view of the causes and effects of the underlying and genuine problems of information security and terrorism.

Prediction about cyberterrorism has become the most powerful mechanism for distortion, establishing the cyberterrorist as a symbol of fear. Such predictions nearly always take the specific form of the future threat scenario. This is subtly different from the type of prediction identified by Cohen, where there is an implicit assumption that recurrence of particular events is inevitable and talk of 'next time' and what to do about it is widespread (Cohen 2002: 26). With the future threat scenario, the future event is not based on past events, but is entirely hypothetical and based on tenuous links made between two or more elements. Hackers have done x so terrorists will do it soon. This

new technology *could* be used by terrorists to do *y*. A new vulnerability discovered in system *z might* be exploited by terrorists. It is implied that the future threat is imminent and that immediate, prescriptive social reaction is necessary. It matters not that these predictions fail to come to fruition. This is either ignored and replaced by fresh claims or used as evidence that action was taken in time to prevent catastrophe. If the prediction has been very specific, such as claims that cyberterrorist attacks were inevitable in reaction to the second war in Iraq, the shortcomings in such a prediction are dismissed with the argument "It didn't happen this time, but it will happen...". The argument is unassailable because it cannot be disproved and fresh reports about new future threat scenarios will soon divert public attention towards other alarming prospects. The parallel distortion of relabelling existing cybercrime and so forth as 'cyberterrorism' serves to keep the sense of fear immediate. Cohen describes the import of this:

> Unlike the case of natural disasters where the absence of predictions can be disastrous, with social phenomena such as deviance, it is the presence of predictions that can be 'disastrous'. (Cohen 2002: 26)

Cohen speaks of self-fulfilling prophecies. Yet the issue with cyberterrorism is not that it will suddenly appear for real, but that such prophecies will lead to fear and consequent changes in social behaviour and will permit justification of excessive social controls.

4. CLAIMS-MAKERS

What Cohen terms 'moral entrepreneurs' will here be called 'claims-makers' since this seems to be a more accurate term for the behaviour discussed in this section. The processual model calls for a separate discussion of claims-makers, experts and the political and media élites, yet a particular feature of the discourse on cyberterrorism is that these categories of actors are almost impossible to separate. Critcher has noted that this can be a problem (Critcher 2003: 152). The stakeholders are easy to identify: politicians, law enforcers and security services, and the information security industry. However, all of these have made claims about cyberterrorism, all have some degree of specific expertise – or at least are accredited with such expertise in the press – and all can be considered élite in some sense, although politicians are more obviously so than the others. Nonetheless, even if the same actors are performing multiple functions, it is still important to attempt to tease out those functions into separate strands. Claims-making activities will, therefore, be discussed in this section, with experts and élite consensus discussed in following sections.

4.1 Orientations

Both US and UK politicians make claims which are widely reported in the UK press. Both countries exhibit similar concerns about the ubiquitous topics of technology and terrorism, especially since 2001, at which time the US experienced a phenomenon well-known to the UK: a terrorist attack on home soil. There is evidence of diffusion of concern manifesting in a trend, but no more than that, for claims made by politicians in the US to be made subsequently by politicians in the UK. Claims of politicians are oriented towards prophecies of doom and disaster and, although they may have specific information which points towards the imminent nature of the threat, they have certainly not intimated in public that such a class of information exists, even if they are precluded from discussing it in detail. They use the rhetoric of fear to highlight vulnerabilities which might be exploited by terrorists, asserting that our society is as much at risk from cyberterrorism as it is from bombers. Politicians have stressed both the networked and interdependent nature of information systems and the apparent ease with which they can be attacked with catastrophic effect. The statements made are always sweeping, over-simplified and lacking in evidence to back them up. The audience is left in no doubt that cyberterrorism is extremely dangerous but, were an interested member of the public to dig a little deeper, he would have extreme difficulty ascertaining how a cyberterrorist attack might actually work. The underlying vision is of the fragility of social order, exacerbated by the addition of another layer to society – cyberspace – which is nebulous, largely unregulable and is beginning to challenge the status quo. The Internet in particular has brought with it enormous benefits for individuals, but represents in many ways a nightmare of destabilisation for the state and a threat to the hegemonic interests of Government. The unison of the twin sites of anxiety of terrorism and the Internet in the concept of cyberterrorism is an attempt at restoring certainty in a period of flux. The fight against a common enemy has that effect. In terms of the relationship between these claims-making politicians and the press, such claims have been extremely influential in sensitising the press to the issue of cyberterrorism and ensuring its high profile. In the cyberterrorism discourse, politicians are leaders, not followers.

Contrary to politicians, law enforcers are concerned with the fine detail of cyber-threats. The findings demonstrate that they are in the business of claims-making, but in a restrained manner. They emphasise that the Internet and related technologies have given rise to new challenges for law enforcement. New crimes, and new ways of committing old crimes, have emerged, but law enforcers lack the skills and resources to tackle them effectively. Overblown images of disaster are rare, but we are given a

picture of a growing problem which will remain unaddressed until such time as law enforcers are properly equipped to deal with it. Law enforcers seem to have a relatively calm attitude towards cyberterrorism and the prevailing view seems to be that this is something for the future. For now, there are more pressing problems of cybercrime and conventional terrorism. As to the latter, law enforcers do make claims about terrorist *use* of ICTs but, again, these claims are tempered with the assessment that the Internet is a double-edged sword: useful to terrorists, but also useful to law enforcers who have a new means of tracking their activities. It is this edge of the sword they seek to sharpen with appeals for enhanced powers of surveillance and investigation.

Of all the claims-makers, the orientations of law enforcers are the most balanced. The discourse of law enforcers is firmly rooted in traditional issues of crime and terrorism. They are, in general, careful not to confound these two issues, which would be a pre-requisite for participation in the cyberterrorist discourse. As a result, law enforcers do not tend to be the source of the more alarmist accounts of cyberterrorism in the press and seem to be operating alongside the media rather than leading it.

Perhaps surprisingly, the information security industry is a late-comer in terms of claims-making which is visible in the press. Not until after publication of the PCCIP report in late 1997 does the industry start to feature to any significant degree. Since it became an active claims-maker, however, the industry has shown itself to be deeply split. One faction claims that cyberterrorism is a serious threat, real and growing. The future threat scenario is used liberally and cyberterrorism is characterised as the 'next, logical step' for terrorists. Security flaws which might be exploited by cyberterrorists are emphasised.

The other faction counter-claims that cyberterrorism is a distraction from the genuine problems of cybercrime and conventional terrorism, although they claim no particular expertise in respect of the latter. They use the language of disruption rather than destruction and stress that successful cyber-attacks require rare skills, often inside information or access, and are unlikely to cause damage on a scale attractive to terrorists. These counter-claims, now representing the majority view in the industry and academic press reviewed in Chapter 2, are attenuated in the national newspapers which favour the minority vision of cyberterrorist disaster scenarios. These scenarios and claims do not reach the stage of emotional or intellectual evaluation of the situation. Prophecies of doom are made, but are not linked to moral and social decline. This is a purely technological perspective. As far as the industry's relationship with the press

goes, a few regular contributors, such as Mi2g, can be identified who seem to have a symbiotic relationship with the press. If a quote is needed to back up a sensational story, they are happy to oblige. In return, the press often publish details of reports drafted by these organisations, raising their public profile and reinforcing their aura of expertise.

The media, in this case specifically the press, are, according to Cohen's formulation of moral panic (2002: xxiv), capable of acting as claims-makers in their own right and such is the case here. In common with politicians and some exponents of the information security industry, images of information system vulnerability are combined with exaggerated and distorted claims about past cyberterrorist attacks and nightmare visions of what will undoubtedly happen in the future. Once again, the view of cyberspace as a force for uncertainly and instability is common, leading to the conclusion that social order is at risk from sociopathic individuals operating outwith the physical restrictions and legal and moral constraints of the real world.

4.2 Images

The claims of politicians and exponents of the information security industry are quite clear that cyberterrorists exist and are responsible for unprecedented threats to information systems. These claims rest on a collection of images relating to who the threatening individuals are and why they are resorting to this behaviour.

Images of vulnerability are important for the construction of the cyberterrorist threat. After all, if there are no vulnerabilities, the threat is largely academic. However, although frequently referred to, these supposed vulnerabilities are rarely described in detail. Security flaws undoubtedly exist, but these are subjects for specialist press, not national newspapers. A general sense is promoted that computers and their systems are full of holes just waiting for exploitation. The ubiquity of Microsoft products and their apparent notoriety for being unstable and insecure plays a part in this perception. The Internet itself is portrayed as insidious, a powerful force in its own right and sometimes even described as having a will of its own. But detail is important. How, for example, is a cyberterrorist located in the Middle East going to reach and then breach the supervisory control and data acquisition (SCADA) systems of a nuclear power station and set off a nuclear explosion? Such systems are not, in fact, connected to public networks like the Internet and are often isolated even from internal networks (Green 2002). Again, the notion that aeroplanes can be made to crash by hacking air traffic control systems is far fetched, to say the least. These systems cannot be accessed from

the Internet and are, in any event, mediated by human beings, the air traffic controller and the pilot, both of whom have eyes in their heads. This, too, is simplistic, but the examples do not need to be more complicated to demonstrate the absurdity of the claims which are routinely presented in the press. These scenarios are repeated time and again, often not just as possibilities but as probabilities. The image of vulnerability gains its force through repetition, not reason.

The image of the perpetrators is constructed on two fronts. On the one side, claims-makers indiscriminately relabel hackers as cyberterrorists and cybercrime as cyberterrorism, although law enforcers are less prone to this. This relabelling applies both to specific incidents and to the community of hackers and their activities more generally. Anything which might be regarded as both technologically-related and in the grey areas of deviant behaviour is liable to be labelled 'cyberterrorism'. As to the reason why hackers would engage in cyberterrorism, this seems to amount to little more than a natural extension of the existing 'criminal' label routinely applied to hackers since the 1980s to the more serious 'terrorist' label. Underlying motivations and the fact that hackers are not trying to coerce governments or intimidate the public are routinely ignored.

On the other side, it is taken for granted that terrorists are engaging in cyberterrorism which is, thereby, instantly conjured into existence. Government politicians have tended to emphasise computer dependence as a self-evident reason for cyberterrorist attack. This argument is sometimes backed up with the reasoning that, as security surrounding more traditional targets gets tighter, terrorists will naturally turn to the 'softer' alternative of cyber-attack. Similar arguments have been made by the military and some in the information security industry, who turn to theories of asymmetric warfare to 'demonstrate' that it is the logical next option for terrorists. The might of conventional Western military force overwhelms the meagre resources of a terrorist group or rogue state, so the latter must inevitably turn towards the asymmetric advantages offered by networked technology, both as a tool and as a target. Such claims ignore the reality that a cyber-attack is neither soft nor easy, with human and technological barriers being virtually insurmountable to anyone but a well-placed insider, yet the image painted is invariably of a terrorist attacking from outside the target entity.

4.3 Causal explanations

Normally, claims-makers in a moral panic would proffer causal explanations for the condition causing concern. These are not easily identified in the cyberterrorism discourse. There is no attempt by claims-makers at socio-cultural explanation of *why* a particular anomic individual would want to perpetrate such an attack or from which social problem he himself suffers which would motivate him to such deviance. 'Facts' are presented instead: the fact of society's technological dependence; of security flaws; of society's vulnerability; of cyberterrorists trying to attack.

Sometimes the Internet is presented as being the 'cause' of cyber-deviance in general and cyberterrorism in particular. This does not advance any rational explanation, it simply permits the grouping together of a raft of undesirable behaviour – hacking, paedophilia, pornography, fraud, theft and terrorism – as evidence that the Internet is somehow immoral in itself for facilitating such behaviour. The closest thing to an explanation is in the notion, discussed above, that it is logical that hacking should escalate to cyberterrorism and it is logical that terrorists should turn to cyberterrorism, either recruiting hackers or developing skills themselves. It is presented as self-evident that terrorists will increasingly turn to cyberterrorism as conventional terrorism becomes harder to execute. Yet there is no sign that the strategy of the suicide bomber is either difficult to execute or anything other than spectacularly successful from the terrorist's point of view. Such an 'explanation' for the phenomenon does not bear even the most cursory scrutiny.

4.4 Interests and exploitation

Claims-makers are "groups organized to make claims about an issue, whose own interests are served by its prominence" (Critcher 2003: 152) and it is important to understand what these interests might be. The interests of claims-makers are rarely made explicit and must be inferred from all the circumstances. Such an analysis should not be approached with cynicism. The motivations of claims-makers may be quite transparent but this does not necessarily mean that their stated beliefs are not sincerely held or that they do not genuinely believe they are acting for the good of society. Nevertheless, claims-making is a rhetorical exercise (Best 1990: 24). Claims-makers give a type of deviance a name, establish it as a threat and advocate solutions. When concern spreads and manifests in the media, this confirms the gravity of the issue. The only evidence presented is supposition and prediction, so the question must arise: what do claims-makers seek to achieve by elevating what is apparently a non-issue to such a

prominent position? Perhaps the real focus is less on the supposed social problem and more on the proposed solution to that problem? It does seem that each major group of claims-maker has something to gain from the 'solution'. The conclusion is that cyberterrorism appears to be constructed exclusively of rhetoric.

It is quite common for politicians to make claims, sometimes individually, sometimes in groups, but it is rather less common for government politicians to be a leading exponent of sensationalised claims about a social problem, as is the case with cyberterrorism. There may be several reasons for this. In common with other governments, the UK Government has exhibited a desire over a number of years to exert increasing control over technology and behaviour in cyberspace by enhancing regulations and introducing new legislation, civil and criminal. This is not necessarily social control for its own sake. Privatisation, deregulation and globalisation of many industries and utilities have resulted in reduced government control over and knowledge of owners and operators of information networks and regulation of the Internet in particular is extremely challenging (Madsen 1996; Rathmell 1999). The Government is now in the position of wanting to reassert control over the telecommunications networks and is facing an uphill struggle against a public whose imagination has been captured by the perceived freedoms offered by the Internet (Madsen 1996). There is a real need for Government to highlight the importance of information security and to encourage those in the private sector to take appropriate defensive measures. This is especially important in respect of systems forming part of the CNI since the majority of these systems and, consequently, their security, rest in the hands of the private sector. It is possible that the cyberterrorism discourse is, in part, an attempt to raise the profile of the need for security and to spur the private sector to further action, although there is scant evidence in the corpus for this proposition.

The criminal angle has a much higher profile. The fight against terrorism, including cyberterrorism, has routinely been used as a justification for increasing levels of social control, particularly in the form of increased powers of intelligence-gathering and investigation for the police and security services. This will be discussed in detail below. It is undoubtedly the case that law enforcers and the Government have, to a certain degree, common interests in this regard. The Government's ambition is to further its anti-terrorism and law and order agendas with increasingly 'tough' measures. To the extent that these measures include enhanced powers for law enforcers which make their difficult job easier, the claims made by both parties have similar ends. It is extremely

significant that arguments about terrorism and cyberterrorism have been used to justify legislation which in fact applies to crime as well as terrorism. Cyberterrorism is used to leverage arguments about social control in another sphere of social policy. Government has a legitimate interest in promoting security and social order, but political emphasis on cyberterrorism is properly labelled 'exploitation' if it obscures appropriate debate about the target issues of information security, law and order.

The natural interests of law enforcers in securing enhanced powers to assist with intelligence and investigation have been noted. There are, however, further considerations relating to remit and resources other than investigatory powers. Responsibility for cybercrime and cyberterrorism has passed through and between several units over the years and it has been a consistent criticism that it is not clear where the lines of responsibility lie. MI5, the National Criminal Intelligence Service (NCIS), a computer crime squad at Scotland Yard, Special Branch and regional police forces all seem to have had a stake. The National Information Security Coordination Centre (NISCC) is also involved in research and intelligence-gathering. The National Hi-Tech Crime Unit was set up in April 2001 and it was hoped at the time that it would permit rationalisation of policing of hi-tech crime. It suffered, however, from under-resourcing and, again, lack of a clear remit. It is now defunct and, along with NCIS, has been absorbed into the Serious Organised Crime Agency (SOCA), set up in April 2006. It remains to be seen if SOCA is capable of achieving the much-needed rationalisation, but this is likely to depend on the one thing which has undoubtedly plagued the police throughout the history of cybercrime investigation: lack of resources. There is insufficient manpower, training and logistical resources to cope with the increasing technological aspects of modern criminal investigation. Although the police and security services tend not to sensationalise their claims, their claims in relation to cyberterrorism have certainly been a part of the campaign to justify both an extended remit and additional resources.

The interests of that faction within the information security industry which advocates the existence of the cyberterrorist threat are more obviously commercial in nature. A large part of this industry's revenue derives from the sale of security solutions, both products and services. Claims about the threat from cyberterrorism seem designed to stimulate greater sales of security products. In addition, companies making such claims often do so by way of publication of security reports which are then taken up by the press. This enhances the public profile of the company and lends an aura of expertise,

discussed further below. Both are commercially valuable and are likely to lead to greater demand for their services. Therefore, it must be admitted that they may have a clear commercial incentive to transmit their concerns about the risks from cyberterrorism. Those taking the contrary view within the industry dismiss this as scaremongering and likely to bring the industry into disrepute. If they are right, potential customers may come to regard information security vendors as cynical exploiters and consequently reduce their demand for goods and services.

5. EXPERTS

Experts are not straightforwardly distinguished from claims-makers. Genuine experts in a moral panic are, in any event, rare and it is much more common for claims-makers to be accredited as experts in order to lend greater weight to their claims, so that expertise is not so much inherent as bestowed by the media and political élites (Critcher 2003: 152). In the case of cyberterrorism, all major claims-makers can lay claim to some degree of expertise. Government politicians can lay claim to a certain expertise on cyberterrorism because they have access to that which most others do not: detailed intelligence on the terrorist threat provided by the police, security services and the military and reports on the security and vulnerability of the CNI. When they claim that terrorists are developing the capability for cyber-attack, it is assumed that they do so with access to classified information and that in itself implies expertise of a sort: they know something others do not. For that reason, weight is accorded to such claims in the press and it is rare for them to be contested. For identical reasons, the police, security services and the military claim, and are considered by the press to have, expertise in matters relating to cyberterrorism.

This is a slightly strange state of affairs, since 'experts' in a moral panic are more normally drawn from relevant professions, pressure groups and the like. Information security professionals are a much better fit in this respect. They claim expertise on information security issues for the logical reason that that is their profession. Those who claim expertise on cyber*terrorism* are perhaps stretching that logic because it is unlikely that they have access either to detailed terrorist intelligence or to studies on CNI vulnerability. Nevertheless, the press is ever-willing to accredit information security professionals with expertise and this applies whichever side of the fence they are on. Claims by those asserting that cyberterrorism is a threat are effectively presented in the press as evidence of the fact. Conversely, the significant minority of press articles which seek to attenuate the threat message use quotes from those on the

other side as a debunking tool. On the basis of literature reviewed in Chapter 2, it is likely that the majority of information security professionals do not view cyberterrorism as a significant and imminent threat, but the views of these experts are not reported in a representative fashion in the national press.

There is another sort of 'expert' used in the press who is never identified except by the characteristic of his own expertise, which readers are asked to accept without question. The classic formulation is "Experts say that..." and then a proposition is made which backs up the whole tenor of the article. This device is widely used in press reports on cyberterrorism to give weight to sensationalist and unsubstantiated claims about the dangers from cyberterrorism. When the views of the unidentified 'experts' are analysed as a whole, it is difficult to find any coherent thread of argument running through their claims. This suggests that such people are of the 'rent-a-quote' variety, who simply reply to questions asked by journalists in the manner best suited to the journalist's purpose. They cannot be considered as a coherent body with a consistent message. Some of these contributors may be academics, others may be unidentified information security professionals, it is not generally clear. Academics, if they can lay claim to expertise on cyberterrorism, are rarely quoted explicitly and, despite the substantial literature on cyberterrorism, cannot be considered to be a meaningful part of the public discourse.

6. ELITE CONSENSUS AND CONCERN

This element of the processual model is not present in Cohen and was added by Critcher as a result of lessons learned from Goode and Ben-Yehuda's attributional model (Critcher 2003: 153). The essential insight is that the support of public opinion is a bonus in a moral panic but not a necessity. If public opinion is needed, it tends to be constructed and invoked by the media. On the other hand, consensus and concern among the political and media élites are essential to a moral panic. Critcher explains:

> In moral panics we have a circuit of communication between the mass media, claims makers and the political elite. If enough of these decide there is an issue and that action is required, a moral panic becomes possible. Conversely, if there are differences of opinion within them, a moral panic is more likely to founder.
>
> ... [T]he media are linked to the elites on whom they report, decide who can join the ranks of this elite and construct for the elite a version of 'the public' who are addressed and invoked but never actually consulted. (Critcher 2003: 138)

There is no indication that the public is unduly concerned about cyberterrorism, certainly not to the point that online behaviour has been modified (Chapter 2, section 8). Nor has the press considered it necessary to construct and invoke such public concern in

its presentation of the cyberterrorist threat. If the intention were to sensitise the public to cyberterrorism, it has been successful insofar as the term 'cyberterrorism' has been accepted into public discourse, but widespread public concern of the sort normally found in a moral panic has not apparently followed.

Concern among the political and media élites is evident, however. The political élite in this case includes both US and UK politicians since the UK press has recognised the claims of both. Concern about cyberterrorism has been something of a self-fulfilling prophecy, with the endless rounds of claims-making, based on distortion, reinforcing and augmenting the concerns expressed in those very claims. Hackers are distorted into cyberterrorists; cybercrime is twisted into cyberterrorism; terrorists must be working on a cyberterrorism programme because it is 'logical' for them to be doing so; each newly discovered information system vulnerability is an inevitable target for cyberterrorism; a successful attack would produce terrible destruction and loss of life. Any related episode might trigger such claims, common examples being the emergence of new computer viruses, arrest or prosecution of a hacker, discovery of a security flaw in a popular product, publication of a new cybersecurity report or the aftermath of a conventional terrorist attack.

After a number of such cycles of claims-making, the threat solidifies and becomes more real. The definition of cyberterrorism becomes clearer and the discourse becomes more consistent, both essential for a moral panic. This is the point at which consensus is reached. Press reports of cyberterrorism had been running for a decade by the time the PCCIP report was published (1997), but this report appeared to herald the first signs of political consensus that the cyberterrorist threat was genuine and that government action – in both the US and UK – was needed. The many devastating terrorist attacks attributed to al Qaeda since then have reinforced this consensus, but in a curiously tangential manner. First, they provided an opportunity for fresh rounds of claims-making based on evidence that al Qaeda operatives used ICTs in the planning phase of these attacks. These claims were based on two types of distortion: the relabelling of the evident terrorist 'use' of ICTs as cyberterrorism; alternatively, the argument that this 'use' was the precursor of what was inevitably to come, viz a full cyberterrorist attack. Second, these events heightened sensitivity to terrorism generally and unrelated, electronic events were drawn into the terrorism net. For example, new virus attacks were attributed to al Qaeda, as was, briefly, the 2003 North American power failures. Further, use of the future threat scenario became more frequent so that the link between

ICTs and terrorism became even stronger. Third, the string of conventional terrorist attacks starting with 9/11 has resulted in a strong consensus that extreme measures are necessary to contain the terrorist threat and the established link between ICTs and terrorism has been a central plank in arguments about exactly what measures are necessary.

The consensus evident in the political and media élites is, therefore, based on distortion of the seriousness of the threat from cyberterrorism, its causes and effects. The cyberterrorist has been brought into sharp focus as an al Qaeda operative with exceptional technical skills who is capable of attacking the CNI in such a way as to produce massive destruction and death. This consensus has been challenged with counter-claims, mostly from within the information security industry: that cyberterrorism does not exist and is not imminent; that hackers, insiders and routine system failures, not terrorists, are the challenge for information security; and that cyber-attacks are not capable of producing the catastrophic results mooted. Nevertheless, these claims are not given prominence in the press and, to use Critcher's formulation, their exponents are not permitted to join the political élite.

A closed discourse has developed, then, agreed by both politicians and the press. The source of the threat has been identified as the triumvirate of hackers, terrorists and ICTs, most prominently the Internet, which have been confounded so consistently that the cyberterrorist has emerged. The nature of the threat is that infrastructure critical to the very operation of society is vulnerable to attack from a single terrorist individual sitting at a computer on another continent. Such an attack is likely to lead to the deaths of innocent citizens and/or destruction which will disrupt lives on a massive scale. Legal and practical measures to protect citizens and punish perpetrators must be developed and the ultimate responsibility for doing this rests with the state and its agents.

7. COPING AND RESOLUTION

This stage in the processual model focuses on the solutions which are advocated to address the problem and by whom, the measures which are actually instigated and whether these legal or procedural innovations turn out to be effective or symbolic.

Obvious *solutions* to the problem are almost never discussed by politicians and law enforcers. They may stand accused of opportunism and scaremongering, but the information security industry is at least promoting something resembling an answer to the problem, that is security products and services. It is self-evident that protecting

systems against hackers, virus attacks and so forth, also protects them against cyberterrorism. The method of attack would be identical, only the intentions behind the attack would be different. Nevertheless, although the claims of the information security industry about the threat from cyberterrorism are highly visible, the proposed solution, their goods and services, are not often explicitly mentioned in the press. Politicians and law enforcers might be expected to promote high standards of information security more vigorously in the circumstances, perhaps by characterising it as a positive civic duty to secure vital networks upon which so many rely. They may even be justified in describing it as a matter of national security. But they do not.

Instead, politicians, and law enforcers to a lesser extent, concentrated on legal proscription. A wide definition of cyberterrorism was incorporated into English law in Section 1 of the Terrorism Act 2000 and individuals suspected and found guilty of the offence are subject to the full might of the anti-terrorism régime. The enactment of legal measures squarely addressing the subject of a moral panic generally heralds a rapid decline in interest about the issue. This was not the case here. Around the time the Act was being debated and for a period after its enactment, there was significant press interest but, contrary to the narrative so far, this interest centred around the view that the definitions in the Act were *too* wide and risked the bizarre situation of hackers – and here the press reverted to hackers' erstwhile image as spotty teenagers – becoming terrorists overnight. The press did not at this point abandon their insistence on the dangers of cyberterrorism, quite the contrary. This legislation was not, however, recognised as being the solution to the problem.

Here were the first signs of the cyberterrorism episode departing from the model moral panic. The Act barely features in the main discourse on cyberterrorism which, it now seems apparent, is about more than the legal recognition of the problem. The key to understanding the social reaction to cyberterrorism is to place it in its rightful position: as the cognitive link between terrorism and technology.

At this point, it is useful to make a brief digression to explore Cohen's deviancy amplification model. This model provides a 'link' between folk devil, in this case hackers and cyberterrorists, and moral panic, although Cohen now acknowledges that the deviancy amplification model is better characterised as a model of causation in a constructionist sense rather than in a positivist sense (Cohen 2002: xxiv). An initial (social structural) problem is addressed by an initial (deviant) solution. The initial (deviant) solution in this case was hacking and the initial problem was not so much a

problem as an opportunity: computers and networks there to be explored, boundaries to be pushed. The societal reaction follows, based on distortion. From hackers to cyberterrorists, the social reaction has now been through several evolutions, but distortion of the seriousness of the issue, its causes and effects, has been a consistent feature throughout. Next comes the operation of the control culture, exploitation and the creation of stereotypes. New police units have been created to combat cybercrime and terrorism, new legislation has been passed to criminalise cyber-deviance and assist the police, there has been evidence of both ideological and commercial exploitation by claims-makers and strong stereotypes have emerged of both hackers and cyberterrorists. The next steps of the deviancy amplification model stipulate polarisation of the deviant group and increased deviance, followed by confirmation of the stereotypes such that the theory on which the social reaction is based appears to be proved. In other words, the definitions of deviance are justified. According to Cohen's revised views, this should not be understood as a literal increase in deviance in response to the social reaction, but as an increase in the number and types of activities which are defined by society as deviant. "For those who define and those who are defined, sensitization becomes a matter of cognitive framing and moral thresholds" (Cohen 2002: xxiv). This is the net-widening effect, by which, in this case, any form of cyber-deviance may be attributed to cyberterrorists and events which would otherwise be ignored attract attention. The real effect of this 'increased deviance' is on the magnitude and scope of the social reaction, not on the deviants themselves. By labelling more and more events and types of activity 'cyberterrorism', more cyberterrorism exists and so the initial concern about it appears to have been merited. This is a departure from the traditional labelling theory to which Cohen originally subscribed.

In fact, the supposed deviants themselves have actually played a surprisingly low-key rôle in the panic about cyberterrorism. Whereas it might be expected that the identification of a social problem and a group of likely culprits would be logically prior to the advocated solution, it seems that in this case a vision of the solution came first and the social problem was constructed to justify that solution. For the solutions advocated in this discourse are not aimed solely at mitigating the problem of cyberterrorism. Cyberterrorism is used as one of a number of justifications for new measures of social control which address the twin evils of terrorism and ICTs. This is another example of how undue emphasis is placed on the use of technology generally. Technology, and the Internet in particular, is a new medium for human interaction, but

without it terrorist organisations would still function as they have always done. Communication, organisation, fundraising through criminal activity, recruitment and propaganda would still take place. Technology does, however, provide terrorists with the benefits of speed and anonymity; it allows propaganda and recruitment drives to reach wider audiences; it obviates the necessity for geographic proximity for the purposes of communication, organisation and fundraising. It is these properties of scale, anonymity and the severing of geographic ties which inspires fear and urgent calls for greater controls over the Internet and other technologies.

So it transpired, that the legislation enacted gives law enforcers and others greater access to electronic information. Data retention provisions, the right to requisition keys to encrypted data and enhanced powers of electronic surveillance have been the most controversial aspects of this legislation. All these measures are geared towards removing or reducing barriers to intelligence gathering and police investigation. The concept of cyberterrorism was an essential tool for justifying these sweeping powers because it had created that all-important link between terrorists and ICTs, particularly Internet communications. By concentrating on eye-catching arguments about terrorists and technology, attention was drawn away from another reality, that these new measures were not restricted just to terrorist activity: they applied equally to ordinary criminal intelligence and investigations.

The findings demonstrate two sides to this rhetorical coin. First, measures which were ostensibly aimed at terrorist activity and were exclusively promoted as such might, through the use of wide definitions, be used in criminal investigations, bringing Draconian measures within the grasp of enforcers of the ordinary criminal law. Second, criminal legislation which really had little to do with terrorism was, nevertheless, promoted by reference to arguments about terrorism, thus distracting legislators and the public from debates about the way in which legislation is really intended to be applied and whether the new law was proportionate or even necessary. A central problem for governments has been how to claw back some control over the Internet. Free flow of information and communications has made the Internet enormously popular with users, but it has become a nightmare for governments and law enforcers who are increasingly anxious to establish mechanisms for surveillance and access to personal records analogous to those long-established in the real world. If control is to be achieved by persuading users that their electronic comings and goings should be overseen rather as if by CCTV, powerful reasons must be given if the public is not to revolt. In the

cyberterrorism discourse, the ubiquitous Internet comes to symbolise moral degeneration and lawlessness, the ubiquitous terrorist threat is blended into the electronic environment and the result appears to be increased vulnerability of individual and state which, in turn, justifies increased powers for police and security services. Herein lies the utility of the concept of cyberterrorism which, from this perspective, is less about cyber-attack and more about terrorist use of technology.

On this view, politicians and law enforcers become the major players in the cyberterrorism discourse because they are framing the desired 'outcomes' which were, in fact, the goal all along. Once the media inventory and sensitisation processes had taken hold, over-estimation of the seriousness, causes and effects of cyberterrorism followed, leading in turn to these escalations in the control culture. This societal control culture operates to construct and then maintain a moral consensus which, in this case, reduces to the idea that too much electronic freedom for society at large is damaging because it allows crime and terrorism to flourish.

8. FADE AWAY

In a moral panic, legal and procedural innovations normally provide a form of narrative closure or, from another perspective, a symbolic resolution (Critcher 2003: 141). It is as if a bubble of hysteria grows, with ever louder calls for "something to be done" and, when something is seen to be done, the bubble is burst, the urgency gone. The issue is forgotten or routinised and other social problems take centre stage. This has not yet happened with cyberterrorism. New legislation has been introduced but it has not brought about narrative closure. The future threat scenario is still strong and the evidence suggests it is still growing in importance year on year. This makes sense if the cyberterrorism discourse is viewed as a tool for strengthening the social control culture rather than a social problem in need of an urgent and focused solution.

Cyberterrorism, then, seems to be established as an enduring focus for claims and news coverage. Periods of greatly increased intensity can be distinguished, tending to suggest that this is not a single, prolonged episode of moral panic, but perhaps a serial panic, rather like the classic paedophilia moral panic (Critcher 2003: 110). The meta-discourses of technology and terrorism as perennial sites of social anxiety have been mobilised and linked by the cyberterrorism panic. The link now established, they provide a stable background against which concern about cyberterrorism may rise up again at any time. It is likely that cyberterrorism is yet to have its day as each successive peak of concern continues an upwards trend (Chapter 5, Figure 2).

9. LEGACY

This study has demonstrated that all the elements for a moral panic about cyberterrorism are in place. A new social problem has been defined and the finger of blame has been pointed. Those responsible have been identified and stereotyped. Politicians, elements of the information security industry, the police and security services have emerged as the groups involved in defining the problem and pronouncing on suitable remedies. Other, usually nameless, individuals have been accredited with expertise by the press. A new, symbolic legal category of cyberterrorism has been created and other solutions have been advocated, almost always involving an increase in the social controls over ICTs, most specifically granting law enforcers increased powers of electronic surveillance, interception and data acquisition. These powers have not been limited to terrorist activity, although the justifications given for them were.

All the elements are in place, except one which has not hitherto formed a part of the processual model: the critical mass in terms of media coverage has not quite reached the level at which it can be said "here is a clear moral panic". This can never be an absolute judgment, but a relative one made with reference to related issues. The related issues, in this case terrorism and hacking, still command more column inches (Figures 3 & 4). High levels of concern about conventional terrorism and hacking, measured in terms of quantity of press coverage, are justified and hardly seem disproportionate. The suicide bomber exists and walks among us. The hacker, in a far less dangerous rôle, continues to be a nuisance, although not much more than that. The cyberterrorist is not yet ready to take centre stage. Rather, he is waiting in the wings, already written into the script, with his lines learned and patiently waiting his turn in the limelight. His cue will be a significant event such as a hack with genuinely catastrophic consequences or the discovery of terrorist plans to carry one out. That may happen next week, or it may never happen.

In one sense, this episode has already served its purpose. Without the need to generate more press coverage, claims-makers have already achieved those measures of social control which they have so far deemed necessary in the fight against terrorist use of technology. They have also achieved the bonus of extending these controls beyond terrorism and into the realms of conventional criminal acts. The need to drive the rhetoric of terrorism and technology further will only be necessary in the future if politicians and others desire to make further inroads into civil liberties of ordinary citizens in the name of law and order and national security.

Society should be extremely cautious about confounding hackers with terrorists and accepting the cyberterrorist construction if we accept that deviance amplification, along the constructionist lines elucidated by Cohen in his later work, is possible. The use of cyberterrorism as a tool to mobilise a combination of the meta-discourses on technology and terrorism has given politicians and law enforcers a justification for taking an expansionist view of the anti-terrorism régime. The approach of policy makers has been "What tools might be needed in the fight against terrorism" rather than "How can we fight terrorism in a manner least likely to infringe the civil liberties of ordinary citizens". In practical terms, allowing the cyberterrorism label to spread to behaviour unrelated to terrorism allows policy makers to apply the Draconian version of social control reserved for terrorists to those who do not merit it. But this is not simply a matter of criminals receiving a harsher version of something they deserve anyway. It is a question of exaggerating, even fabricating, the scope and scale of a serious problem in such a way as to persuade the *innocent* to compromise something precious: their freedoms.

It is possible that the harm caused by cyberterrorism may spread further than this. The tendency of a moral panic is to confuse through over-simplification and distortion rather than to illuminate. If the public are induced to focus on cyberterrorism, there is a danger that other, more serious and immediate problems may be allocated a lower priority than they merit. Although hackers, and now cyberterrorists, are the public face of information insecurity, the greater problem lies within organisations. Threats from insiders, both innocent mistakes and malicious damage, and routine system failures remain a far greater headache for most information security officers. Information security professionals, deemed experts by virtue of their profession, tread a fine line between hyping the hacker myth to gain business and remaining competitive in the market place by giving sensible advice and practical solutions to businesses who know where the real problems lie.

Whether or not this episode qualifies as a moral panic, the result has been the same: the imperative to reduce complex arguments to simplicity has the effect of distorting the public's capacity for understanding. I have argued that the social control culture has operated to establish and maintain the moral consensus that too much electronic freedom is a bad thing because it allows crime and terrorism to flourish; and that society must inevitably accept curtailment of civil liberties and individual privacy in order that criminals and terrorists may be thwarted. This all sounds very cynical and it would be if

the primary goal of politicians and law enforcers were to limit the freedoms of citizens and increasingly to control their everyday activities. Yet I do not think that this is their goal. I think it has come to be considered the inevitable and necessary consequence of a genuine desire to protect the public from crime and terrorism. It is a fine distinction, but a vital one. There is nothing wrong with the desire to protect the public, indeed it is what society expects of its leaders and their agents. What *is* wrong, is the price society is asked to pay for this goal and I conceptualise the price as those restrictions on civil liberties and personal privacy. The mistake is to stifle debate on what is the right price to pay. Politicians and the press have acted systematically to stifle such debate and evidence for this can be found in the small-scale but oft-repeated claims about the dangers from cyberterrorism to the grand-scale suppression of the views of the privacy lobby over ID cards. The fault lies equally with the public who allow this debate to be stifled, who do not question the lazy argument of those who confound cybercrime with terrorism and who stare with bovine indifference whilst their freedoms are cut away.

CHAPTER 10

CONTRIBUTIONS AND FUTURE DIRECTIONS

The assertions of claims-makers who argue that cyberterrorism is the next 'logical' step for terrorists are important because they highlight an implicit defect in social understanding. These ideas hark back to the work of academics who have analysed the cyberterrorist threat using models based on rational choice theory (Rabbie 1991; Devost, Houghton et al. 1996; Giacomello 2004). Such analyses, based as they have been in the positivist paradigm, concentrate on predicting behaviour within a relatively deterministic framework of assumptions about patterns of social behaviour. The interpretative assumptions underlying this study lead to a contrary view, that prediction of human behaviour with any degree of accuracy is exceptionally difficult since there is a high level of indeterminacy in social processes characterised by free will. 'Rational choice' in the sense used by Rabbie et al. has nothing to do with how individuals, in this case terrorists and hackers, understand the world because it does not address the cognitive and evaluative processes specific to them. Rather, these choices are only 'rational' from an objective, disconnected perspective. Such claims may highlight the *possibility* of a future course of action, but they say nothing about its likelihood. This is why the academic fields of terrorism and information security are desperately in need of interpretivist study into the actions and motivations of would-be attackers. It also explains why there is a dearth of such studies: some degree of access to the relevant individuals would be a prerequisite, but such research subjects are unlikely to grant access willingly. These research aims are almost impossible to operationalise without unacceptable risk to the researcher.

This study has taken a different approach. By espousing a constructivist perspective within the interpretative paradigm, it has taken a first step towards an understanding of where the concept of cyberterrorism comes from. On this view, positivist perspectives on the 'rational choices' of a deviant group become less important than an understanding of how deviance is first constructed then reacted to in a social context. This does not fill the gap just identified, but it does make a contribution towards a socio-cultural understanding of the perception of technological risk at the very highest

levels of society. The argument that cyberterrorism is socially constructed forces a reconsideration of the assumptions of risk on which policy-making is currently based.

As technology becomes further integrated in the socio-cultural landscape, it is increasingly important to show how technological risk is constructed and not just experienced. This has far-reaching implications, and the case of cyberterrorism is only one case in point. The discourses which have been alluded to in this study are just part of a process of negotiation over where the line should be drawn between the rights and freedoms of individuals on the one hand and the exercise of social control by the state on the other. This is not a new debate, of course, but it has intensified with the arrival of the so-called Information Society.

As this discourse evolves, as it assuredly will in the coming years, it needs to be informed by a deeper understanding, not only of how technology changes the characteristics of the risk to society from hostile actors, but also of how society itself constructs and manages that risk and the effects of this on the construction and positioning of moral boundaries. This discourse is still in its early stages and it is important that there is an open, meaningful and informed debate about how society should look. Constructs such as cyberterrorism, having no settled definition and confounding so many distinct issues, should not be allowed to obfuscate the real issues. Simply put, careless use of terminology impedes understanding, communication, sense-making and, ultimately, affects both the justifiability and ultimate efficacy of policy decisions. Forming policy to counter a phenomenon which is insufficiently understood may result in rules which either do not address the issue adequately or overextend the law into areas where it is not warranted. The extension of the social control culture into the electronic environment is inevitable but how it is done and how far it goes are still questions subject to debate. This debate would be greatly clarified if the definition of cyberterrorism developed in this study (Chapter 2, Section 2.4), or something like it, were adopted and, in this limited sense at least, this study has been able to identify a problem and propose a possible solution. It is, however, clear that social perspectives on technology, risk and morality are vast substantive areas in need of a concentrated research effort in the coming years to supplement the existing literature in this area so that academics can offer their ideas and help to inform the debate.

This study has focused on the stereotypes, images and symbols employed in the discourses associated with cyberterrorism. These have a wider importance than that hitherto identified, because they determine at a fundamental level how the problem is

characterised. If the problem is characterised as quasi-military and a threat to national security, as seems to be the case at present with cyberterrorism, then high levels of social control are indicated, with a centralised, government-led approach. If, on the other hand, the problem is characterised as one of information and organisational security, as is the case with hacking, then it is more appropriate for individuals and organisations to take responsibility for their own defensive strategies and there is a less obvious rôle for state intervention. The central importance of the use of stereotypes, images and symbols in characterising a social problem in this way is addressed by a variety of models of social problem construction, already well-developed in reference disciplines such as Sociology. The Information Systems domain has a long history of turning to the reference disciplines for its theoretical foundations, particularly when faced with the need to "address one of the most troublesome issues of the field, namely the reconciling of the technical and the social, the 'hard' and the 'soft'" (Avgerou 2000). Arguments about consolidating the discipline of Information Systems should not be allowed to get in the way of the fertile exchange of ideas between this discipline and others (Keen 1980; Benbasat and Weber 1996; Robey 1996). This study has pioneered the use of the moral panic concept, borrowed from Sociology, in the Information Systems domain and it is hoped that the benefits of this approach have been made manifest.

As well as providing a theoretical explanation of the social processes at work in the particular case of the social construction of cyberterrorism, the findings of this study have also contributed to the wider debate on moral panic by adding another case to the literature, discussing the relevance and usefulness of the moral panic framework and making some modest suggestions for modification. The latest evolution of the processual and attributional models of moral panic as developed by Critcher (2003) are, themselves, relatively untested. They have been used together in this study in an innovative way, the attributional model to organise the findings and the processual model to guide the discussion. This has worked particularly well as a research strategy and helped to prevent the researcher from becoming overwhelmed by the sheer volume of information. The addition of the meta-principles for interpretative research in the IS domain elucidated by Klein and Myers (1999) and the use of grounded theory methods has enhanced scientific rigour in the course of a long and arduous period of research and made sense of the use of moral panic as an heuristic device within the interpretative tradition. Some would argue that this approach has been at the cost of the purity of the

grounded theory method which is demanded by scholars such as Glaser (eg 1992), although Strauss and Corbin do allow the use of their version of grounded theory methods in this way, albeit that this is probably at the far end of the scale of uses which they do permit (1998: 49 et seq). With these modifications, this study may be added to the evidence of Critcher (2003: 178), that the usefulness of the decades-old concept of moral panic to social science is not yet spent.

Nevertheless, this study has other limitations, many of which flow from the choice of corpus of data and the method of analysis used. First, because of practical limitations of time and resources, data was gathered only from the national press and no primary sources relating to any of the claims-makers – apart from the press itself – were consulted. This means that the findings of this study are, in part, based on claims made by third parties which are filtered, reported and interpreted by the press before they are interpreted by the researcher. Although the findings of this study are grounded in the available data, they can only go so far in making claims about the totality of the discourse on cyberterrorism. This approach has been justified with reference to arguments about the centrality of the media rôle in a moral panic (see further Chapter 3). Realistically, however, the findings are limited to that part of the discourse which appears in the UK national press and generalisability of the specific findings in relation to the case of cyberterrorism is compromised to that extent.

There is no doubt that the findings and discussion would have carried more weight had there been an opportunity to incorporate systematically other sources of data, such as interviews with the public, information security trade publications, police publications and political sources, much as Cohen did in his study of Mods and Rockers (2002). It is clear that future research might fruitfully analyse such alternative data sources using similar research methods to those used in this study. This would, to a certain extent, remedy the bias knowingly introduced into this study because a shortage of time and resources precluded a wider variety of data sources. This broader approach to data gathering would also make a valuable contribution, not only to moral panic research, but also to the wider field of socio-technical research which deals with public perceptions of technology.

Nevertheless, the broader findings about the use and applicability of moral panic as an heuristic device are more easily generalisable than those specific findings about the case of cyberterrorism. Critcher correctly objects that the processual model of moral panic is vague about both the triggers for and decline of moral panics. He further suggests that

it is necessary to specify which discourses are evident in a moral panic and their relationship to perceptions of risk. It appears that the latter suggestion may in fact be a partial remedy to the former objection. Discussion of underlying discourses can be incorporated, as indeed they were in this study, into a wider view of what should be included at certain stages of the processual model particularly 'emergence' and 'legacy'. Moral panics do not spring out of the ether. They are rooted in their historical context and generally, as Critcher's work demonstrates, emerge out of one or more existing discourses. Once a moral panic has run its course, its legacy may be to "produce such changes as those in legal and social policy or even in the way the society conceives itself" (Cohen 2002: 1), so contributing towards a change in the underlying discourse. This may be achieved in the course of one panic, or it may require several, loosely related panics. Critcher detects a shift in the underlying discourse in moral panics from youth in the 1960s and 1970s to childhood in the 1980s and 1990s (Critcher 2003: 155). Cohen detected a shift in the underlying discourse from offender and the criminal justice system to victim (Cohen 2002: xxiv). This study of cyberterrorism has identified another possible shift, from technology as benign and enabling to technology as dangerous and a source of vulnerability. It also seems likely that the transformation of the hacker into the cyberterrorist parallels a shift in the wider discourse in society from law and order issues to questions of national security. There is a wealth of Information Society issues here which have not hitherto been investigated in detail and might be taken up by scholars in that field.

This study could have been set up in a number of different ways using different research methods, although a different approach would inevitably lead to a change of emphasis in the findings and conclusions of the study. An interesting future direction for this work would be to triangulate the findings of this study by employing alternative techniques to link the corpus of data to the moral panic framework in order to establish whether the same or similar findings would result. This would certainly address one of the fundamental problems with this type of research, that of the deep immersion of the researcher in the research material and the inevitable interplay between that material and the researcher's interpretation of it. However careful the researcher is to achieve a balance between objectivity and sensitivity to the subject (Strauss and Corbin 1998), for both researcher and reader, the difficulty in ascertaining the extent to which the researcher has been successful remains. A separate study of the same corpus using a different research method and, perhaps, a different researcher would not only add depth

to the findings and conclusions of this study but would also serve either to verify or to challenge its results. Either outcome would be valuable to research in this field, either by adding weight to existing research or adding a different perspective to the same problem.

Two possible methodological candidates, Critical Discourse Analysis and content analysis, were identified in Chapter 4 as alternatives to the Grounded theory approach used in this study. A study of this corpus of data using content analysis techniques from a positivist perspective would certainly be an interesting exercise and would provide an alternative viewpoint. Moral panic research has historically been located in the positivist paradigm as well as the interpretative, and the comparison would be an illuminating one.

Moving sideways into the critical tradition, the use of CDA is likely not only to be helpful in cross-checking the results of this study but would also take it on to the next analytic level. It should be made explicit that the use of the concept of underlying discourses in this study, whilst important, has been tangential to the main thrust of the research. This is emphatically only a first step in demystifying a topic, cyberterrorism, and its related concepts as identified using a grounded theory approach Discourses relevant to the cyberterrorism debate have been identified but not analysed in any detail. Simply put, this study has not set out to achieve an analysis of the discourses involved in cyberterrorism: it has merely identified those discourses as being present and in need of further research. A logical next step would be to go further and examine the language used in the context of a true discourse analysis using CDA.

Moral panic was chosen as a framework for this study for the reasons discussed in Chapter 3. However, other frameworks could have been chosen and might usefully be followed up in future research as a means of complementing and, perhaps, verifying the findings of this study. It was decided at an early stage that the concept of the public perception of risk would not necessarily be a primary focus of this study, although it does arise as one issue amongst many others. Future research might fruitfully explore this area in more detail. For example, the Social Amplification of Risk Framework (Kasperson, Kasperson et al. 2003) is increasingly popular within the Information Systems domain. It was noted in Chapter 3 that SARF considers how risk communication interacts with social, psychological, institutional and cultural processes to produce interpretations of risk and that there are close parallels with deviance definition. The fact that SARF is primarily concerned with risk contrasts nicely with

moral panic, which places greater importance on morality. Perception and acceptance of risk is so often tied to a process of blaming, and a SARF study of cyberterrorism would complement nicely the obvious moral dimension of blaming which is better highlighted by moral panic.

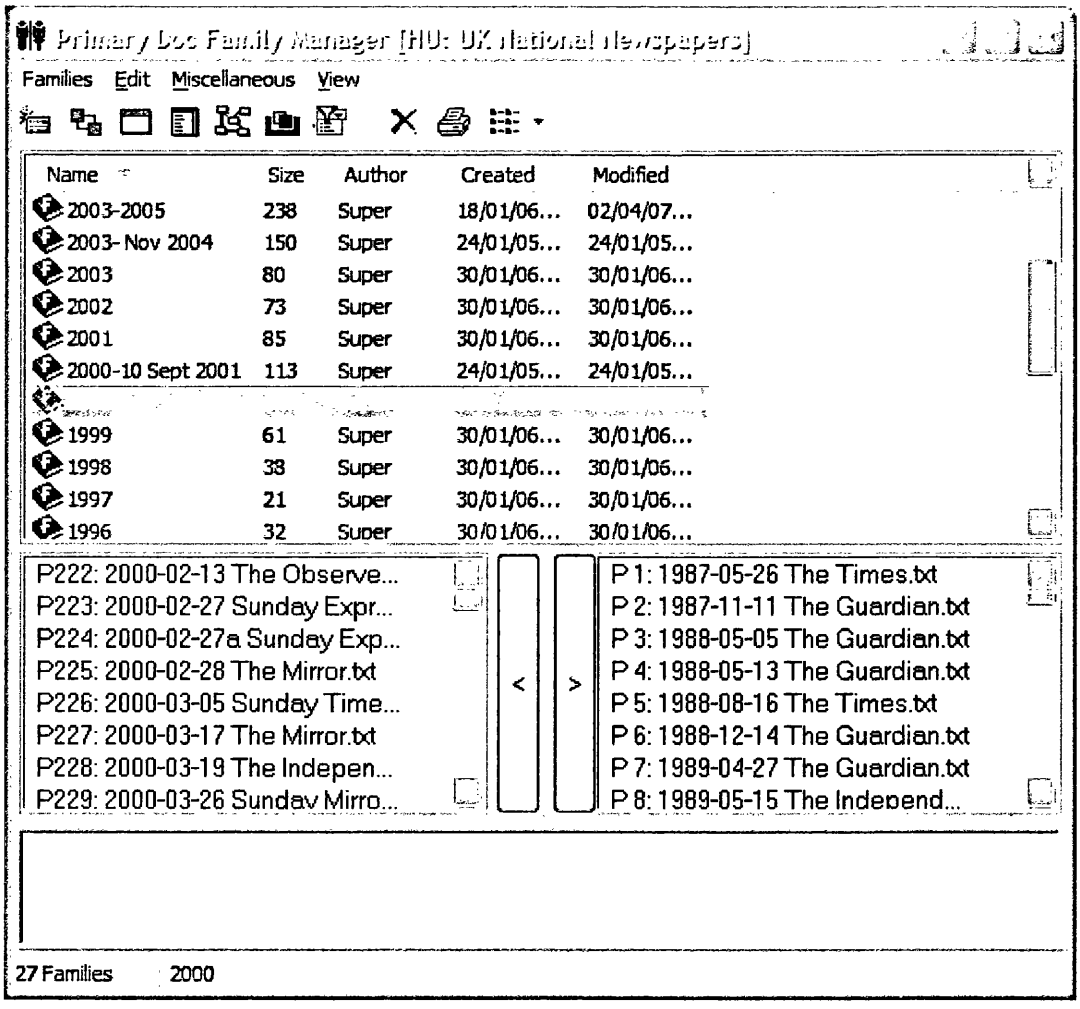
If the findings of this study are not sensational, that is all to the good: it is hoped that one of its central contributions will be to show how the debate on cyberterrorism should be moved away from the sensational, back to a more level-headed discussion where political transparency and rational argument can be promoted. At the end, there are two certainties about cyberterrorism. First, to this day, there are still no publicly documented cases of the real thing. Second, cyberterrorism will continue to make the headlines. A paper tiger indeed.

APPENDIX: THE USE OF ATLAS/TI

The building blocks of grounded theory are facilitated by Atlas/ti. In order to supplement the explanations given in Chapter 4, this Appendix aims to provide pictorial examples of how the analysis was carried out.

Primary documents

The primary texts themselves were ordered and separated into family groups. This facility was used to categorise the texts according to date and publication (ie the newspaper the article came from). Each entry in the two middle boxes in the picture below represents a primary document, in this case a newspaper article. Each document name shows the primary document number (Px – ie P1 to P681, since there are 681 articles in this corpus of data); the date of the article in the format yyy-mm-dd; and the publication, eg The Times.

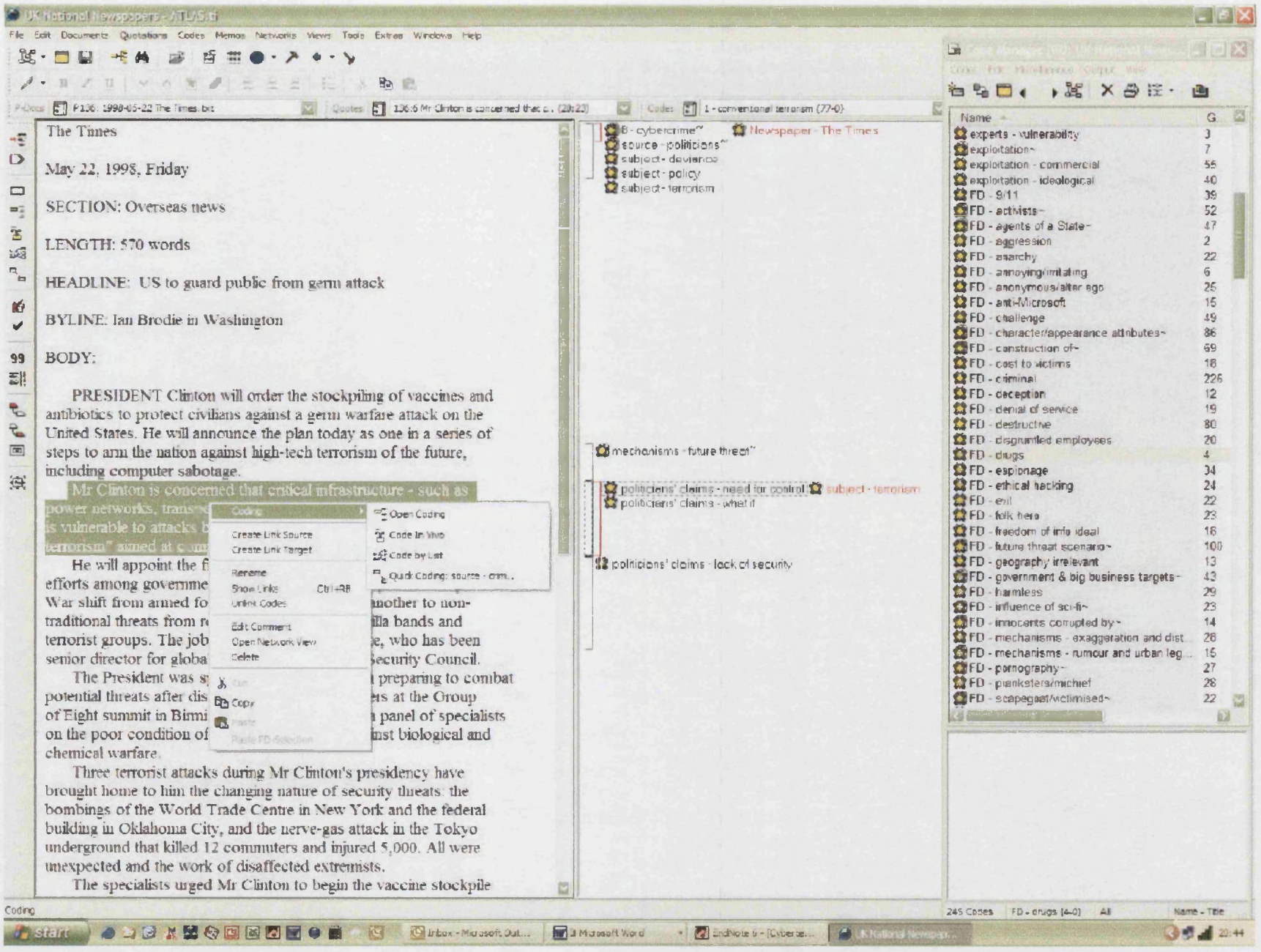


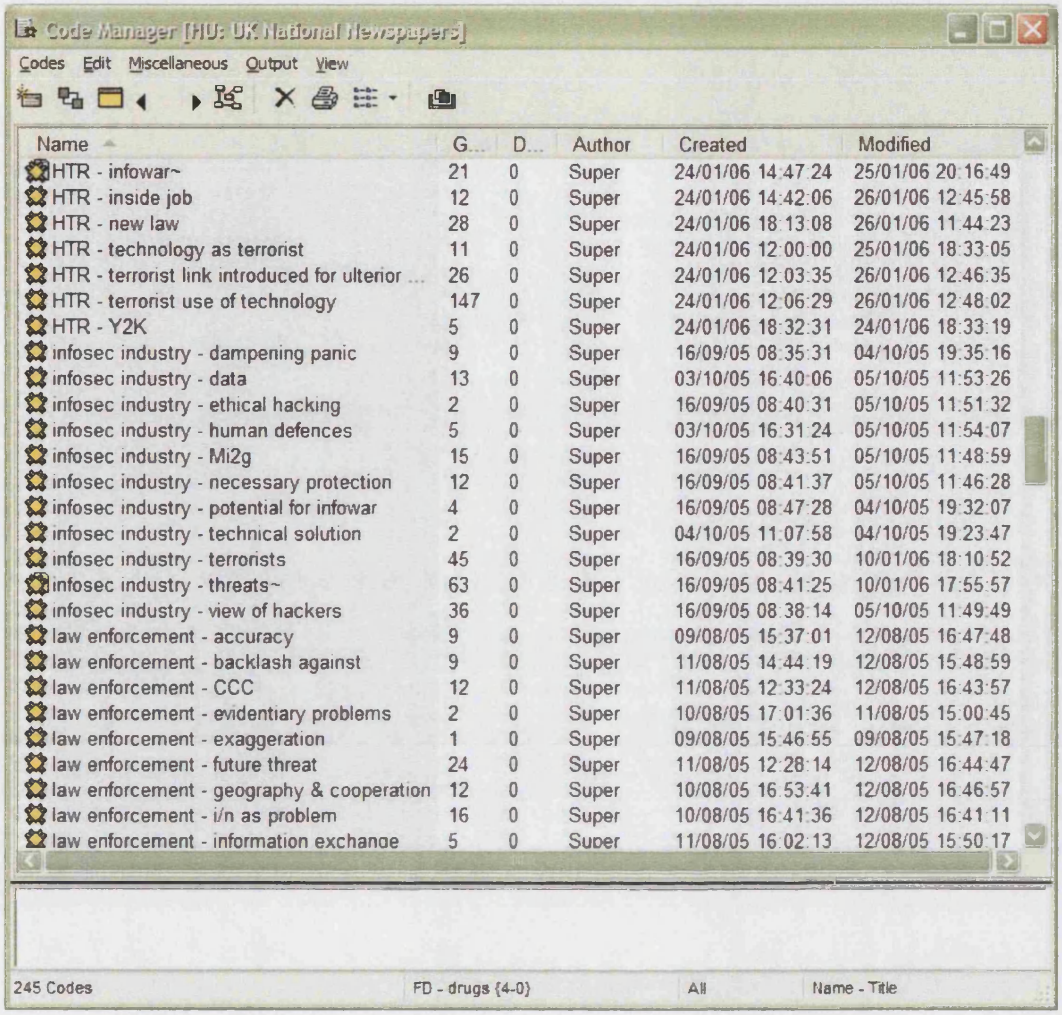
In the example above, the names of the document families are displayed in the top box. In this case, the document family names are all dates because time periods were particularly significant in this study. All the texts from the year 2000 family have been retrieved and are displayed in the middle box on the left. The box on the right contains all the texts which do not belong to this family. The empty box at the bottom is used for memos should the researcher wish to record any, although none was necessary here. At the bottom of the window, the programme notes that there are 27 families of primary documents in all and that the one currently being displayed is the family called "2000".

Coding

A variety of different coding techniques are called for by Strauss and Corbin (1998) in order to build grounded theory: open coding, axial coding, selective coding and coding for process. The differences between these types of coding are facilitated in Atlas/ti, although the researcher needs to be very experienced with the software in order to grasp all the nuances. There are several ways to code in Atlas/ti. First, one can perform open coding by highlighting text and attaching to it whatever new code the researcher chooses. Second, one can perform in vivo coding, in which the text selected becomes the name of the code itself. Third, one can code by list, so that a right click brings up the available codes which have been used before (or only a family of codes if the researcher is performing axial or selective coding) and the researcher can attach one or more of those codes. As the researcher reaches saturation of each theoretical category, this will become the most used method of coding. Finally, the quick coding function allows the researcher to attach a specific code to a sequence of quotations – particularly useful for selective coding.

The screenshot on the following page shows the main workspace of Atlas/ti, with a window overlaid on the right hand side which contains a full list of all the codes in use. In this example, a passage in an article from The Times on 22 May 1998 (the left side of the workspace) has been highlighted and, with a right click of the mouse, the available coding options are displayed. To the right of the Times article is the window which displays the codes which have already been attached to quotations from the document.


The Times
May 22, 1998, Friday
SECTION: Overseas news
LENGTH: 570 words
HEADLINE: US to guard public from germ attack
BYLINE: Ian Brodie in Washington
BODY:
PRESIDENT Clinton will order the stockpiling of vaccines and antibiotics to protect civilians against a germ warfare attack on the United States. He will announce the plan today as one in a series of steps to arm the nation against high-tech terrorism of the future, including computer sabotage.
Mr Clinton is concerned that critical infrastructure - such as
Coding
Create Link Source
Create Link Target
Rename
Show Links Ctrl+RB
Unlink Codes
Edit Comment
Open Network View
Delete
Copy
Open Coding
Code In Vivo
Code by List
Quick Coding: source - crim...
Newspaper - The Times
mechanisms - future threat
politicians' claims - need for control
subject - terrorism
politicians' claims - what if
politicians' claims - lack of security
Three terrorist attacks during Mr Clinton's presidency have brought home to him the changing nature of security threats: the bombings of the World Trade Centre in New York and the federal building in Oklahoma City, and the nerve-gas attack in the Tokyo underground that killed 12 commuters and injured 5,000. All were unexpected and the work of disaffected extremists.
The specialists urged Mr Clinton to begin the vaccine stockpile

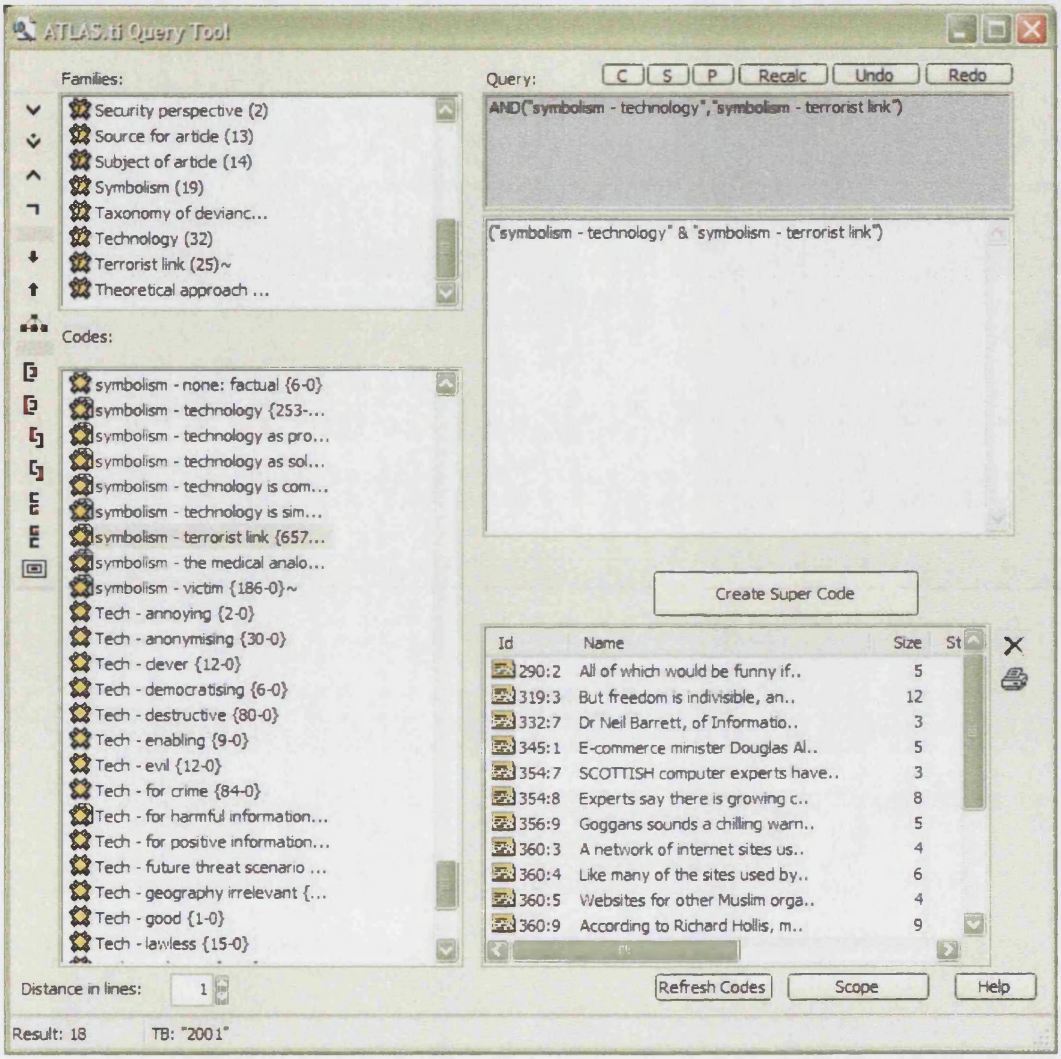


The picture above is a detail of the code manager window. There are 245 codes in all (see bottom left), which is a very large number but this is accounted for by the fact that they are effectively arranged into code families by name. The codes starting with *HTR* are sub-categories of the *HTR* category, which stands for "hacker-terrorist relationship". Likewise, the individual codes commencing with *infosec industry* and *law enforcement* are sub-categories of that parent category. This dual-naming system was simply a work-around developed by the researcher because she found it necessary to add a third level of analysis to the two basic levels provided by Atlas/ti. The number of times each code has been applied to a segment of text appears as the number to the immediate right of each code and this is used as a measure of theoretical significance of each code/concept.

Quotation retrieval

The findings chapters are presented in the form of a narrative which weaves in and out of quotations from the corpus. It was possible to retrieve all the segments of text which

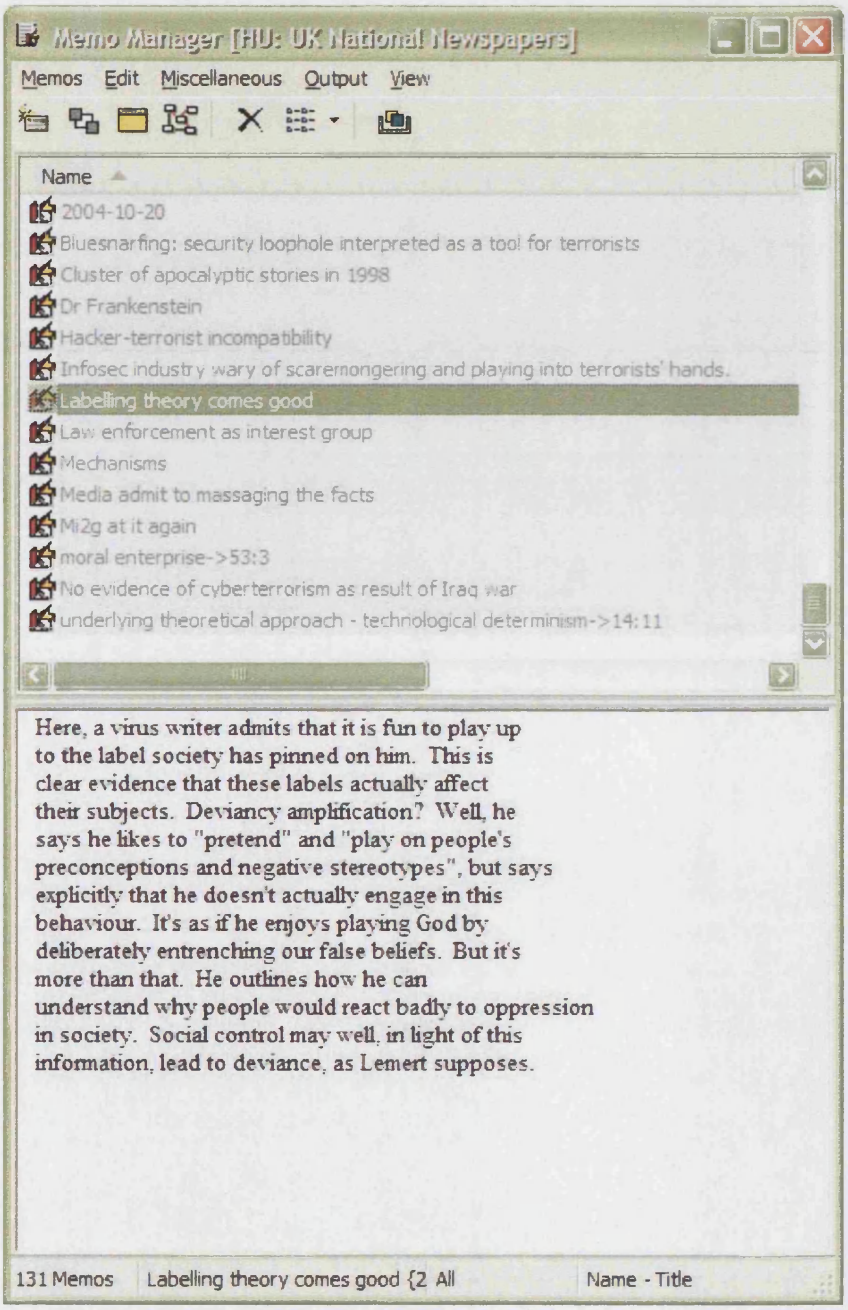
were coded with a particular code by double clicking on the relevant code in the code manager window. A more complex retrieval process could be constructed using the query tool.



This example shows a relatively simple query. Only articles from the year 2001 were searched (the reference to TB: "2001" at the bottom of the window). From the codes list (bottom left window) the codes *symbolism – technology* and *symbolism – terrorist link* were combined in a Boolean AND search (the technical form of the search query is shown in the grey window, top right). All the quotations which answer this query are listed in the bottom right window and we can see from the bottom left of the workspace that there are 18 of these quotations. If this combination of search terms is considered to be theoretically significant, it is possible to compile the results into a "super code" so that they are instantly retrievable in the future under a specific code/concept name. Again, this technique is particularly useful for axial coding.

Memos

The following is a screenshot of the Memo Manager window from which all the memos recorded during the analysis process can be accessed. A total of 131 memos were recorded and, in accordance with the strategies described by Strauss and Corbin (1998: see, for example, Chapter 14) many of them were integrated into the theoretical explanation set out in the findings and discussion chapters.



The memo highlighted here records my thoughts at the time I came across some quotations from a hacker who was discussing his motivations for writing viruses. Reading this passage triggered in my mind a strong association with the deviancy amplification model described by Cohen which was based on Lemert's idea that the notion that social control might lead to deviance is potentially a richer premise for deviancy research than the notion that deviance leads to social control. These ideas are discussed in more detail in Chapter 3.

A complete list of codes used

1 - conventional terrorism
10 - communication
11 - ethical hacking
12 - information warfare
13 - hoax
2 - c tool; d target
3 - d tool; c target
4 - cyberterrorism
5 - conventional crime
6 - c tool; d target
7 - d tool; c target
8 - cybercrime
9 - accidental damage
empirical evidence
experts - anonymity
experts - comments on others' motivations
experts - control of Internet
experts - culture of fear
experts - cyberwar
experts - data
experts - future threat
experts - hackers' motivations
experts - hackers becoming militant
experts - Internet communication/democracy
experts - nature of threat
experts - pundits & their motivations
experts - solutions
experts - surveillance society
experts - terrorists
experts - vulnerability exploitation
exploitation - commercial
exploitation - ideological
FD - 9/11
FD - activists
FD - agents of a State
FD - aggression
FD - anarchy
FD - annoying/irritating
FD - anonymous/alter ego
FD - anti-Microsoft
FD - challenge
FD - character/appearance attributes
FD - construction of
FD - cost to victims
FD - criminal
FD - deception
FD - denial of service
FD - destructive
FD - disgruntled employees
FD - drugs
FD - espionage
FD - ethical hacking
FD - evil
FD - folk hero
FD - freedom of info ideal
FD - future threat scenario
FD - geography irrelevant
FD - government & big business targets
FD - harmless
FD - influence of sci-fi
FD - innocents corrupted by
FD - mechanisms - exaggeration and distortion
FD - mechanisms - rumour and urban legend

FD - pornography
FD - pranksters/mischief
FD - scapegoat/victimised
FD - self-regulation
FD - show-off
FD - skill - high
FD - skill - low
FD - students
FD - terrorist
FD - threat
FD - vandals/saboteurs
FD - victim non-reporting
FD - vigilante movement
FD - young
HTR - 9/11
HTR - activism
HTR - association
HTR - attribution of extreme powers to hackers
HTR - authorities' pursuit of Tts
HTR - criminals labelled 'cyberterrorists'
HTR - cyberterrorism exists
HTR - cyberterrorism suspected
HTR - fiction
HTR - future threat scenario
HTR - hackers adopting the Tt label
HTR - hackers coopted by State
HTR - hackers coopted by terrorists
HTR - hackers labelled 'terrorists'
HTR - hackers threatening anti-terrorist systems
HTR - hacking as a terrorist cause
HTR - hacking is NOT terrorism
HTR - infowar
HTR - inside job
HTR - new law
HTR - technology as terrorist
HTR - terrorist link introduced for ulterior motives
HTR - terrorist use of technology
HTR - Y2K
infosec industry - dampening panic
infosec industry - data
infosec industry - ethical hacking
infosec industry - human defences
infosec industry - Mi2g
infosec industry - necessary protection
infosec industry - potential for infowar
infosec industry - technical solution
infosec industry - terrorists
infosec industry - threats
infosec industry - view of hackers
law enforcement - accuracy
law enforcement - backlash against
law enforcement - CCC
law enforcement - evidentiary problems
law enforcement - exaggeration
law enforcement - future threat
law enforcement - geography & cooperation
law enforcement - i/n as problem
law enforcement - information exchange
law enforcement - lack of reporting
law enforcement - need for new law & power
law enforcement - new unit
law enforcement - on FDs
law enforcement - resourcing issues

law enforcement - secrecy
law enforcement - terrorism
law enforcement - turf war
law enforcement - use of i/n by l/e
mechanisms - appeal to 9/11 and 7/7
mechanisms - association
mechanisms - dampening panic
mechanisms - dramatization
mechanisms - exaggeration / distortion
mechanisms - future threat
mechanisms - misdirection of reaction
mechanisms - rumour and urban legend
mechanisms - sensitisation
media claims - agency empire building
media claims - misleading
media claims - potential
media claims - security risk
media claims - sensationalism
media claims - talking up hacker skills
media role - agenda setting
media role - claims-making
media role - image transmission
moral boundaries
moral enterprise
Newspaper - Daily Mail
Newspaper - Daily Telegraph
Newspaper - Financial Times
Newspaper - Mail on Sunday
Newspaper - Sunday Times
Newspaper - The Times
politicians' claims - 9/11
politicians' claims - cyberterrorism
politicians' claims - denying security breach
politicians' claims - developing intelligence necessary
politicians' claims - govt use of IW
politicians' claims - lack of security
politicians' claims - need for control
politicians' claims - need for secrecy
politicians' claims - prescience
politicians' claims - privacy not at risk
politicians' claims - threat overstated
politicians' claims - what if
real-virtual world tension
security - social approach
security - technical approach
source - (ex-)hackers
source - commentary piece
source - commercial sector
source - criminal justice system
source - experts
source - infosec industry
source - law enforcement & security services
source - media
source - other interest groups
source - politicians
source - public
source - public body
source - victim
subject - activism
subject - asymmetry
subject - censorship / freedom of speech
subject - deviance
subject - experts' opinions
subject - fiction
subject - information warfare/espionage
subject - law enforcement

subject - policy
subject - privacy
subject - secrecy
subject - social anxiety and fear
subject - social reaction
subject - terrorism
supertech
symbolism - 9/11
symbolism - anonymity
symbolism - courts and criminal justice system
symbolism - experts
symbolism - Government
symbolism - hacker
symbolism - insects
symbolism - interest groups
symbolism - IT dependence
symbolism - law enforcement
symbolism - none: factual
symbolism - technology
symbolism - technology as problem
symbolism - technology as solution
symbolism - technology is complex
symbolism - technology is simple
symbolism - terrorist link
symbolism - the medical analogy
symbolism - victim
Tech - annoying
Tech - anonymising
Tech - clever
Tech - democratising
Tech - destructive
Tech - enabling
Tech - evil
Tech - for crime
Tech - for harmful information/communication
Tech - for positive information/communication
Tech - future threat scenario
Tech - geography irrelevant
Tech - good
Tech - lawless
Tech - malicious
Tech - medical analogy
Tech - offensive weapon
Tech - powerful
Tech - sophisticated
Tech - terrorist
Tech - use by authorities
Tech - use by terrorists
Tech - vulnerability
underlying theoretical approach - social determinism
underlying theoretical approach - social shaping
underlying theoretical approach - technological determinism

REFERENCES

Allen, J., S. Forrest, et al. (2005). Fraud and technology Crimes: findings from the 2002/03 British Crime Survey and 2003 Offending, Crime and Justice Survey. London, Home Office.

Anderson, E. L. (2002). "Assessing the Risks of Terrorism: A Special Collection of Perspectives Articles by Former Presidents of the Society for Risk Analysis." Risk Analysis **22**(3): 401-2.

APIG (2003). Communications data: report of an inquiry by the All Party Internet Group. London, APIG: 1-39.

Arquilla, J. (2000). "SCREEN SAVER The U.S. government is frantically preparing for the threat of cyberterrorism. And its preparations won't do any good." New Republic(4450): 16-7.

Arquilla, J. and D. Ronfeldt (1999). "The Advent of Netwar: Analytic Background." Studies in Conflict and Terrorism **22**(No. 3, Special Issue: Netwar Across the Spectrum of Conflict): 193-206.

Arquilla, J., D. Ronfeldt, et al. (2000). "Information-Age Terrorism Cyberterrorism continues to capture the popular imagination but the real revolution in unorthodox information-age warfare is the rise of netwar." Current History **99**(636): 179-85.

Astley, W. (1985). "Administrative Science as Socially Constructed Truth." Administrative Science Quarterly **30**: 497-513.

Avgerou, C. (2000). "Information systems: what sort of science is it?" Omega **28**(5): 567-79.

Ballard, J. D., I G. Hornik, et al. (2002). "Technological Facilitation of Terrorism: Definitional, Legal, and Policy Issues." American Behavioral Scientist **45**(6): 989-1016.

Ballesteros, G. (2001). Cyber-terrorism and Information Security, SANS Institute (SysAdmin, Audit, Network, Security) www.sans.org. **2003**.

Bauer, M. (2000). Classical Content Analysis: A Review. Qualitative researching with text, image and sound : a practical handbook. M. Bauer and G. Gaskell. London, SAGE: 131-151.

Bauer, M. and B. Aarts (2000). Corpus Construction: a Principle for Qualitative Data Collection. Qualitative researching with text, image and sound : a practical handbook for social research. M. Bauer and G. Gaskell. London, SAGE: 19-37.

Becker, H. (1966). Introduction. Social Problems: A Modern Approach. H. Becker. New York, John Wiley.

Becker, H. S. (1963). Outsiders : studies in the sociology of deviance. London, Free Press of Glencoe.

Benbasat, I. and R. Weber (1996). "Research commentary: rethinking "diversity" in Information Systems research." Information Systems Research **7**(4): 389-99.

Best, J. (1990). Threatened Children: Rhetoric and Concern about Child Victims. Chicago, University of Chicago Press.

Boni, B. (2001). "Cyber-terrorists and Counter Spies." Network Security **2001**(12): 17-8.

Bowden, C. (2002). "CCTV for inside your Head: Blanket Traffic Data Retention and the Emergency Anti-Terrorism Legislation." Computer and Telecommunications Law Review **8**(2): 21-4.

Bray, J. (2002). Tackling the sources of conflict: what can companies do? The Unlikely Terrorists. R. Briggs. London, Foreign Policy Centre: 78-89.

Bronskill, J. (2001). "CSIS on alert for cyber saboteurs: spy agency monitors threat to computer networks." Ottowa Citizen **2001**(9 January): A3.

Brown, M. (1996). The Revolution in Military Affairs: The Information Dimension. Cyberwar : security, strategy, and conflict in the information age. A. D. Campen, D. H. Dearth and R. T. Goodden. Fairfax, Va., AFCEA International Press: 31-52.

Brull, S. and J. Wagley (2001). "Cyberwar-ready September 11 brought a low-tech surprise attack. Financial industry security strategists don't want to be caught napping for what might come next: information warfare and cyberterrorism." Institutional Investor- International Edition- **2001**(11): 43-8.

Brunskill, B. (2002). The emergence of new threats: cyber terrorism. The Unlikely Terrorists. R. Briggs. London, Foreign Policy Centre: 19-30.

Bryman, A. (2001). Social Research Methods. Oxford, Oxford University Press.

Bunker, R. (2000). "Weapons of Mass Disruption and Terrorism." Terrorism and Political Violence **12**(1): 37-46.

Charmaz, K. (2000). Grounded Theory: Objectivist and Constructivist Methods. Handbook of qualitative research. N. K. Denzin and Y. S. Lincoln. Thousand Oaks, Calif., London, Sage Publications.

Chermak, S. and A. Weiss (2005). "Maintaining legitimacy using external communication strategies: An analysis of police-media relations." Journal of Criminal Justice **33**(5): 501-12.

Cilluffo, F. and C. Gergely (1997). "Information warfare and strategic terrorism." Terrorism and Political Violence **9**(1): 84-94.

CIO Insight (2004). Security and Privacy: Do You Feel More Secure Than Last Year?, www.cioinsight.com.

Cohen, S. (1972). Folk Devils and Moral Panics: the Creation of the Mods and Rockers. London, MacGibbon and Kee.

Cohen, S. (2002). Folk Devils & Moral Panics: the Creation of the Mods and Rockers, 3rd Ed. London, Routledge.

Conway, M. (2002). "Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet." First Monday **7**(11).

Conway, M. (2002a). "What Is Cyberterrorism?" Current History **101**(659): 436-42.

Cover Story (2001). "Cover Story: Operation Internet Injustice." Financial Director: 38-42.

Cresson Wood, C. (2001). "What do the recent terrorist attacks mean for the American information security profession?" Computers & Security **20**(8): 667-70.

Crilley, K. (2001). "Information Warfare: new battlefields, terrorists, propaganda and the Internet." Aslib Proceedings **53**(7).

Critcher, C. (2003). Moral Panics and the Media. Buckingham, Philadelphia, Open University Press.

Crocco, T. E. (2004). "Inciting Terrorism on the Internet: An Application of Brandenburg to Terrorist Websites." Saint Louis University Public Law Review **23**: 451-84.

CSI/FBI (2005). CSI/FBI Computer Crime and Security Survey 2005, CSI.

Cumming, R. (2005). Responses to the growing threat of online terrorism and crime, PITCOM 14 March 2005, KableNET.com.

Czinkota, M. R., G. A. Knight, et al. (2005). "Positioning terrorism in management and marketing: Research propositions." Journal of International Management **11**(4): 581-604.

Danitz, T. and W. Strobel (1999). "The Internet's Impact on Activism: The Case of Burma." Studies in Conflict and Terrorism **22**(No. 3, Special Issue: Netwar Across the Spectrum of Conflict): 257-69.

Dartnell, M. (1999). "A Legal Inter-Network for Terrorism: Issues of Globalization, Fragmentation and Legitimacy." Terrorism and political violence **11**(4): 197-208.

David, M. W. and K. Sakurai (2003). Combating Cyber Terrorism: Countering Cyber Terrorist Advantages of Surprise and Anonymity. International conference on advanced information networking and applications, Xian, China, Los Alamitos Calif.

Davies, R. (2002). An evolution of terror: extreme events and Al Qaida. The Unlikely Terrorists. R. Briggs. London, Foreign Policy Centre: 8-18.

Deisler, P. F. (2002). "A Perspective: Risk Analysis as a Tool for Reducing the Risks of Terrorism." Risk Analysis **22**(3): 405-14.

Denning, D. (2000). "Activism, Hacktivism and Cyberterrorism." Computer Security Journal **16**(3): 15-36.

Denning, D. (2000a). Cyberterrorism. Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services, US House of Representatives.

Desmedt, Y. (2002). "Is there a Need for Survivable Computation in Critical Infrastructures?" Information Security Technical Report **7**(2): 11-21.

Desouza, K. and T. Hensgen (2003). "Semiotic emergent framework to address the reality of cyberterrorism." Technological Forecasting & Social Change **70**: 385-96.

Desouza, K., W. Koh, et al. (2006). "Information technology, innovation and the war on terrorism." Technological Forecasting & Social Change **Article in press**.

Desouza, K. C. (2005). "Restructuring government intelligence programs: A few good suggestions." Government Information Quarterly **22**: 342-53.

Desouza, K. C. and T. Hensgen (2003a). "Every citizen a missile: the need for an emergent systems approach by law enforcement." Government Information Quarterly **20**(3): 259-80.

Devost, M., B. Houghton, et al. (1996). Information Terrorism: can you trust your toaster?, www.terrorism.com: 1-16.

Devost, M., B. Houghton, et al. (1997). "Information Terrorism: Political Violence in the Information Age." Terrorism and Political Violence **9**(1): 72-83.

Devost, M., B. Houghton, et al. (1997a). "Response to Cilluffo and Gergely." Terrorism and Political Violence **9**(1): 95-7.

Devost, M., B. Houghton, et al. (1997b). Organizing for Information Warfare: "The truth is out there", www.terrorism.com: 1-12.

Devost, M. and N. Pollard (2002). Taking cyberterrorism seriously, Terrorism Research Center, www.terrorism.com: 1-3.

Dhillon, G. and J. Backhouse (2001). "Current directions in IS security research: towards socio-organizational perspectives." Information Systems Journal **11**: 127-53.

Dwan, B. (2001). "Cyber-terrorism - Virtual for Who?" Computer Fraud and Security **2001**(11): 12-4.

Embar-Seddon, A. (2002). "Cyberterrorism: Are We Under Siege?" American Behavioral Scientist **45**(6): 1033-43.

Farrell, M. (2003). IS security post 9/11: private affair or public policy? LSE Department of Information Systems Security Colloquia, London School of Economics.

Fay, B. (1987). An Alternative View: Interpretive Social Science. Interpreting Politics. M. Gibbons. New York, New York University Press: 82-100.

FBI (2005). 2005 FBI Computer Crime Survey.

Feinberg, L. E. (2002). "Homeland security: implications for information policy and practice-first appraisal." Government Information Quarterly **19**(3): 265-88.

Foltz, C. B. (2004). "Cyberterrorism, computer crime, and reality." Information Management and Computer Security **12**(2): 154-66.

Forcht, K. A. and J. Pierson (1994). "New Technologies and Future Trends in Computer Security." Industrial Management and Data Systems **1994**(8): 30.

FSA (2006). Financial Risk Outlook 2006, www.fsa.gov.uk.

Furnell, S. M. and M. J. Warren (1999). "Computer Hacking and Cyber Terrorism: The Real Threats in The New Millennium?" Computers and Security **18**(1): 28-34.

Galliers, R. (1985). In search of a paradigm for Information Systems research. Research Methods in Information Systems. E. Mumford, R Hirschheim, G. Fitzgerald and A. Wood-Harper.

Galliers, R. (1991). Choosing appropriate Information Systems research approaches: a revised taxonomy. Information Systems research: contemporary approaches and emergent traditions. H.-E. Nissen, H. Klein and R. Hirschheim.

Galliers, R. and F. Land (1987). "Choosing appropriate Information Systems research methodologies." Communications of the ACM **30**(11): 900-2.

Garrick, B. J. (2002). "Perspectives on the Use of Risk Assessment to Address Terrorism." Risk Analysis **22**(3): 421-4.

Gellman, R. (2002). "Perspectives on privacy and terrorism: all is not lost-yet." Government Information Quarterly **19**(3): 255-64.

George, B. and N. Whatford (2002). Overcoming the threat: public-private partnership. The Unlikely Terrorists. R. Briggs. London, Foreign Policy Centre: 59-69.

Giacomello, G. (2004). "Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism." Studies in Conflict and Terrorism **27**(5): 387-408.

Gilmore Commission (2000). Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. Second Annual Report: toward a national strategy for combating terrorism, Written by RAND personnel.

Gilmore Commission (2001). Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. Third Annual Report: for Ray Downey, Written by RAND personnel.

Gilmore Commission (2002). Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. Fourth annual report: implementing the national strategy, Written by RAND personnel.

Glaser, B. G. (1992). Basics of Grounded Theory Analysis: Emergence vs. Forcing. Mill Valley, CA, Sociology Press.

Glaser, B. G. and A. L. Strauss (1967). The discovery of grounded theory : strategies for qualitative research. Hawthorne, N.Y, Aldine de Gruyter.

Goode, E. and N. Ben-Yehuda (1994). Moral panics : the social construction of deviance. Cambridge, Massachusetts, Blackwell.

Goodman, S., J. Kirk, et al. (2006). "Cyberspace as a medium for terrorists." Technological Forecasting and Social Change **Article in press**.

Gordon, A. (2005). "Terrorism as an Academic Subject after 9/11: Searching the Internet Reveals a Stockholm Syndrome Trend." Studies in Conflict and Terrorism **28**: 45-60.

Gordon, S. and R. Ford (2002). "Cyberterrorism?" Computers and Security **21**(7): 636-47.

Green, J. (2002). "The Myth of Cyberterrorism." Washington Monthly **34**(11): 8-13.

Griffith, D. A. (1999). "Organizing to Minimize a Cyber-Terrorist Threat." Marketing Management **8**(2): 9-16.

Haimes, Y. Y. and T. Longstaff (2002). "The Role of Risk Analysis in the Protection of Critical Infrastructures Against Terrorism." Risk Analysis **22**(3): 439-44.

Halbert, D. (1997). "Discourses of Danger and the Computer Hacker." Information Society **13**(4): 361-74.

Halchin, L. E. (2002). "Electronic government in the age of terrorism." Government Information Quarterly **19**(3): 243-54.

Hall, S., C. Critcher, et al. (1978). Policing the crisis : mugging, the state, and law and order. London, Macmillan.

Harper, D. (2003). "Re-examining cyber security." Industrial Distribution **92**(3): 81.

Harreld, H. and B. Fonseca (2001). "Guarding against cyberterrorism." www.infoworld.com **2001**(22 October): 35-7.

Harvey, F. (2002). "Hacked off by the hype about cyber terrorism." The Engineer **2002**(22 Nov - 5 Dec): 25.

Hawkins, H. S. (2005). "A Sliding Scale Approach for Evaluating the Terrorist Threat over the Internet." George Washington Law Review **73**: 633-48.

Hensgen, T., K. C. Desouza, et al. (2003). "Playing the "cyber terrorism game" towards a semiotic definition." Human Systems Management **22**(2): 51-62.

Hinde, S. (2000). "Smurfing, Swamping, Spamming, Spoofing, Squatting, Slandering, Surfing, Scamming and Other Mischiefs of the World Wide Web." Computers and Security **19**(4): 312-20.

Hinde, S. (2001). "Incalculable potential for damage by cyber-terrorism." Computers and Security **20**(7): 568-72.

Hinde, S. (2003). "Cyber-terrorism in context." Computers and Security **22**(3): 188-92.

Hoffman, B. (1994). Responding to Terrorism Across the Technological Spectrum, RAND Corporation.

Hosein, I. (2006). Briefing for Members of the European Parliament.

Hosein, I. and E. A. Whitley (2002). "The regulation of electronic commerce: learning from the UK's RIP act." Journal of Strategic Information Systems **11**(1): 31-58.

Hunt, A. (1997). "'Moral panic' and moral language in the media." British Journal of Sociology **48**(4): 629-48.

Ingles-Le Nobel, J. (1999). "Cyberterrorism hype." Janes Intelligence Review **11**(12): 48-52.

Internet Governance Project (2005). Political oversight of ICANN: a briefing for the WSIS Summit, www.internetgovernance.org.

Iqbal, M. (2004). "Defining Cyberterrorism." John Marshall Journal of Computer and Information Law **22**: 397-408.

Jenkins, P. (1998). Moral panic : changing concepts of the child molester in modern America. New Haven, CT, Yale University Press.

Jones, A. (2005). "Cyber terrorism: fact or fiction." Computer Fraud and Security **2005**(6): 4-7.

Jones, D. (2002). "Semantic Attacks - A New Wave of Cyber- terrorism." Network Security(3): 13-5.

Jordan, T. (2001). "Mapping Hacktivism." Computer Fraud and Security **2001**(4): 8-11.

Kasperson, J. X., R. E. Kasperson, et al. (2003). The social amplification of risk: assessing fifteen years of research and theory. The social amplification of risk. N. F. Pidgeon, R. E. Kasperson and P. Slovic. Cambridge, Cambridge University Press: 13-46.

Keegan, C. (2002). "Cyber-terrorism risk." Financial Executive **18**(8): 35-7.

Keen, P. (1980). MIS research: Reference disciplines and a cumulative tradition. Proceedings of the First International Conference on Information Systems, Philadelphia.

Kelle, U. (2000). Computer-Assisted Analysis: Coding and Indexing. Qualitative researching with text, image and sound : a practical handbook for social research. M. Bauer and G. Gaskell. London, SAGE: 282-98.

Kincaid, H. (1996). Philosophical foundations of the social sciences : analyzing controversies in social research. Cambridge [England] ; New York, NY, USA, Cambridge University Press.

King, P. (2003). Cyberterrorism. PITCOM. London, KableNET.com.

Kirk, M. (2001). Cyberterrorism: basic components of defense, SANS GIAC (Global Information Assurance Certification) www.giac.org. **2003**.

Kjaerland, M. (2006). "A taxonomy and comparison of computer security incidents from the commercial and government sectors." Computers & Security **Article in press**: 1-17.

Klein, H. and M. Myers (1999). "A set of principles for conducting and evaluating interpretive field studies in Information Systems." MIS Quarterly **23**(1): 67-94.

Kovacich, G. L. and A. Jones (2002). "What InfoSec professionals should know about information warfare tactics by terrorists." Computers and Security **21**(1): 35-41.

Kshetri, N. (2005). "Pattern of global cyber war and crime: A conceptual framework." Journal of International Management **11**(4): 541-62.

Kshetri, N. (2005a). "Information and communications technologies, strategic asymmetry and national security." Journal of International Management **11**(4): 563-80.

Lawson, S. (2002). Information Warfare: An Analysis of the Threat of Cyberterrorism Towards the US Critical Infrastructure, SANS Institute, www.sans.org.

Lee, A. (1991). "Integrating positivist and interpretive approaches to organizational research." Organization Science **2**(4): 342-65.

Lee, E. and L. Leets (2002). "Persuasive Storytelling by Hate Groups Online: Examining Its Effects on Adolescents." American Behavioral Scientist **45**(6): 927-57.

Leivesley, S. (2002). The impact on the business community: building resilience against chemical, biological, nuclear, radiological, explosives and electronic attacks. The Unlikely Terrorists. R. Briggs. London, Foreign Policy Centre: 31-42.

Lemert, E. M. (1951). Social pathology : a systematic approach to the theory of sociopathic behavior, McGraw-Hill.

Lemert, E. M. (1972). Human deviance, social problems, and social control. Englewood Cliffs ; (Hemel Hempstead), Prentice-Hall.

Lemos, R. (2002). What are the real risks of cyberterrorism?, ZDNet, www.zdnet.com.

Levin, B. (2002). "Cyberhate: A legal and Historical Analysis of Extremists' Use of Computer Networks in America." American Behavioral Scientist **45**(6): 958-88.

Lewis, J. (2002). Assessing the risks of cyber terrorism, cyber war and other cyber threats, Center for Strategic and International Studies: 1-12.

Lewis, J. A. (2005). "Aux armes, citoyens: Cyber security and regulation in the United States." Telecommunications Policy **29**(11): 821-30.

M2.com (2002). "New survey examines cyberterrorism concerns." Internet Business News **2002**(16 September): at www.allbusiness.com.

Madsen, W. (1996). "Securing Access and Privacy on the Internet." Computer Fraud and Security **1996**(1): 9-18.

Mahmood, C. (2001). "Terrorism, Myth, and the Power of Ethnographic Praxis." Journal of Contemporary Ethnography **30**(5): 520-45.

Marlin, S. (2001). "Recovery plans prove effective in disaster." Bank Systems and Technology **38**(11): 9.

McFeatters, A. (2001). "Cyber-enemy: America's newest threat is lurking behind computer screens." Pitsburgh Post-Gazette: E3.

McRobbie, A. and S. L. Thornton (1995). "Rethinking `moral panic' for multi-mediated social worlds." British Journal of Sociology **46**(4): 559.

Meehan, M. (2001). "Is Carnivore dangerous? Controversy continues." Computerworld **34**(50): 24.

Merl, S. R. (2001). "Internet Communication Standards for the 21st Century: International Terrorism Must Force the U.S. to Adopt "Carnivore" and New Electronic Surveillance Standards." Brooklyn Journal of International Law **27**(1): 245-84.

Meyer, M. (2001). Between theory, method, and politics: positioning of the approaches to CDA. Methods of critical discourse analysis. M. Meyer. London, SAGE: 14-31.

Middlemiss, J. (2003). "Security: The threat of terrorism, specifically cyber-terrorism, is demanding attention." Wall Street and Technology **21**(Supp): 42-4.

Mingers, J. (2001). "Combining IS research methods: towards a pluralist methodology." Information Systems Research **12**(3): 240-59.

Mingers, J. (2001a). "The paucity of multimethod research: a review of the IS literature." Information Systems Research **12**(3): 1-25.

Moeller, S. D. (1999). Compassion fatigue : how the media sell disease, famine, war, and death. New York ; London, Routledge.

Nader, J. C. (1998). Prentice Hall's illustrated dictionary of computing. Sydney; London, Prentice Hall.

National Statistics (2006). Information and Communication Technology (ICT): Activity of UK Businesses, 2005, www.statistics.gov.uk/pdfdir/intc0207.pdf.

National Statistics (2007). First Release: Internet Connectivity, December 2006, www.statistics.gov.uk/pdfdir/intc0207.pdf.

Neumann, W. (1989). "Parallel Content Analysis: Old Paradigms and New Proposals." Public Communication and Behavior 2: 205-289.

Neville-Jones, P. (2003). Cyber terrorism: a bigger threat than e-crime? PITCOM. London, IAAC.

News (2001). "IT giants team up to fight threat of `cyber-terrorism`." Computer Fraud and Security(2): 3.

Newton, S. (2002). Can Cyberterrorists Actually Kill People?, SANS Institute (SysAdmin, Audit, Network, Security) www.sans.org. **2003**.

Orlikowski, W. and J. Baroudi (1991). "Studying information technology in organizations: research approaches and assumptions." Information Systems Research **2**(1): 1-27.

Paul, L. (2001). When Cyber Hacktivism Meets Cyberterrorism, SANS Institute (SysAdmin, Audit, Network, Security) www.sans.org. **2003**.

PCCIP (1997). The Case for Action: The Report of the Presidential Commission on Critical Infrastructure Protection.

Pollitt, M. (1998). "Cyberterrorism - Fact or Fancy?" Computer Fraud and Security **1998**(2): 8-10.

Post, J., K. Ruby, et al. (2000). "From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism." Terrorism and Political Violence **12**(2): 97-122.

Pounder, C. (2002). "Anti-Terrorism Legislation: The Impact on The Processing of Data." Computers and Security **21**(3): 240-5.

Presidential Decision Directive 63 (1998). White paper: the Clinton Administration's Policy on Critical Infrastructure Protection.

Prichard, J. J. and L. E. MacDonald (2004). "Cyber Terrorism: A Study of the Extent of Coverage in Computer Security Textbooks." Journal of Information Technology Education **3**: 279-89.

PWC/DTI (2004). Information Security Breaches Survey 2004. London, PriceWaterhouseCoopers.

Rabbie, J. (1991). "A Behavioural Interaction Model: Toward a Social-Psychological Framework for Studying Terrorism." Terrorism and Political Violence **3**(4): 134-63.

Rathmell, A. (1997). "Cyber-terrorism: the shape of future conflict?" RUSI Journal **1997**(October): 40-6.

Rathmell, A. (1999). "International CIP Policy: Problems and Prospects." Information Security Technical Report **4**(3): 28-42.

Rathmell, A. (2002). Briefing note to House of Commons Defence Select Committee: enquiry into defence and security of the UK. House of Commons Defence Select Committee.

Rathmell, A. (2003). "Controlling Computer Network Operations." Studies in Conflict and Terrorism **26**(3): 215-32.

Raymond, E. S. and G. L. Steele (1996). The New hacker's dictionary. Cambridge, Mass; London, MIT Press.

Reid, E. (1997). "Evolution of a body of knowledge: an analysis of terrorism research." Information processing and management **33**(1).

Reinares, F. (1998). "Democratic Regimes, Internal Security Policy and the Threat of Terrorism." Australian Journal of Politics and History **44**(3): 351-72.

Richardson, L. (1999). "Terrorists as Transnational Actors." Terrorism and political violence **11**(4): 197-208.

Robey, D. (1996). "Research commentary: diversity in information systems research: threat, promise, and responsibility." Information Systems Research **7**(4): 400-8.

Rogers, M. (2003). The Psychology of Cyber-Terrorism. Terrorists, Victims and Society: psychological perspectives on terrorism and its consequences. A. Silke. Chichester, John Wiley & Sons.

Rombel, A. (2001). "Internet Security in an Insecure World." Global Finance **15**(13): 28-32.

Rombel, A. (2002). "Wiring Government Technology vendors are mining a new IT gold mine, as Uncle Sam opens his wallet to stop cyber-terrorism, and e-government sweeps Europe." Global Finance **16**(2): 40-2.

Ronfeldt, D. (1999). "Netwar Across the Spectrum of Conflict: An Introductory Comment." Studies in Conflict and Terrorism **22**(No. 3, Special Issue: Netwar Across the Spectrum of Conflict): 189-92.

Saiban, J. and J. Sykes (2002). "UK Anti-Terrorism Act 2001 & ISP's." Computer Law and Security Report **18**(5): 338-9.

Sandywell, B. (2006). "Monsters in cyberspace cyberphobia and cultural panic in the information age." Information Communication and Society **9**: 39-61.

Schell, B. and J. Dodge (2002). The Hacking of America: who's doing it, why and how. Westport, CT, Quorum Books.

Schultz, E. (2003). "Cyberterrorism: real threat, or paper tiger?" Computers & Security **22**(1): 2-3.

Schwartau, W. (2000). "Asymmetrical Adversaries." Orbis **44**(2): 197-205.

Scraton, P. (1999). Hillsborough : the truth. Edinburgh, Mainstream.

Seifert, J. W. (2002). "The effects of September 11, 2001, terrorist attacks on public and private information infrastructures: a preliminary assessment of lessons learned." Government Information Quarterly **19**(3): 225-42.

Senia, A. (2001). "Bulletproof your clients' networks." Varbusiness **17**(22): 43-4.

Shaw, E. (2006). "The role of behavioural research and profiling in malicious cyber insider investigations." Digital Investigations **3**(1): 20-31.

Shneiderman, B. (2002). "ACM's Computing Professionals Face New Challenges." Communications- Acm **45**(2): 31-4.

Shockwavewriter (2000). "Is it Cyber-Terrorism, Techno-Terrorism, or None of the Above?" Computer Fraud and Security **2000**(7): 18-20.

Simpson, P. (2003). "Is the threat of cyberterror genuine?" Computer Weekly **2003**(13 March): 22.

Singh, S. (1999). The code book : the science of secrecy from ancient Egypt to quantum cryptography. London, Fourth Estate.

Skibell, R. (2002). "The myth of the computer hacker." Information, Communication & Society **5**(3): 336-56.

Smith, J. (2002). The company response to emerging terrorist threats. The Unlikely Terrorists. R. Briggs. London, Foreign Policy Centre: 43-51.

Spich, R. and R. Grosse (2005). "How does homeland security affect U.S. firms' international competitiveness?" Journal of International Management **11**(4): 457-78.

Stanton, J. J. (2002). "Terror in Cyberspace: Terrorists Will Exploit and Widen the Gap Between Governing Structures and the Public." American Behavioral Scientist **45**(6): 1017-32.

Strauss, A. L. and J. Corbin (1990). Basics of qualitative research : grounded theory procedures and techniques. London, Sage Publications.

Strauss, A. L. and J. Corbin (1998). Basics of qualitative research : techniques and procedures for developing grounded theory. Thousand Oaks, Sage Publications.

Swire, P. (2001). "New anti-terrorism law poses old risks." Counterpunch **2001**(24 October): www.counterpunch.org/.

Thompson, K. (1998). Moral panics. London, Routledge.

Ungar, S. (2001). "Moral panic versus the risk society: the implications of the changing sites of social anxiety." British Journal of Sociology **22**(2): 271-91.

Valeri, L. and M. Knights (2000). "Affecting Trust: Terrorism, Internet and Offensive Information Warfare." Terrorism and Political Violence **12**(1): 15-36.

van Leeuwen, T. (1993). "Genre and field in critical discourse analysis." Discourse and Society **6**(1): 81-106.

Vatis, M. (2001). Cyber Attacks During The War on Terrorism: a predictive analysis, Institute for Security Technology Studies at Dartmouth College: 27.

Veness, D. (2002). The role of the Police. The Unlikely Terrorists. R. Briggs. London, Foreign Policy Centre: 52-8.

Verdict (2006). e-Retail 2006, www.verdict.co.uk.

Waddington, P. (1986). "Mugging as a moral panic: a question of proportion." British Journal of Sociology **37**(2): 245-59.

Walden, I. (2005). "Crime and Security in Cyberspace." Cambridge Review of International Affairs **18**: 51-68.

Walker, C. (2000). "Briefing on the Terrorism Act 2000." Terrorism and Political Violence **12**(2): 1-36.

Walsham, G. (1993). Interpreting information systems in organizations. Chichester, Wiley.

Walsham, G. (1995). "The emergence of interpretivism in IS research." Information Systems Research **6**(4): 376-94.

Wehde, E. (1998). "US vulnerable to cyberterrorism." Computer Fraud and Security **1998**(1): 6.

Weimann, G. (2005). "Cyberterrorism: The Sum of All Fears?" Studies in Conflict and Terrorism **28**: 129-50.

Whine, M. (1999). "Cyberspace - A New Medium for Communication, Command and Control by Extremists." Studies in Conflict and Terrorism **22**(No. 3, Special Issue: Netwar Across the Spectrum of Conflict): 231-45.

Whine, M. (1999a). "Islamist Organizations on the Internet." Terrorism and Political Violence **11**(1): 123-32.

Whitley, E. A. and I. Hosein (2005). "Policy discourse and data retention: The technology politics of surveillance in the United Kingdom." Telecommunications Policy **29**(11): 857-74.

Williams, E. (2002). "Climate of Fear: Cyberterrorism fears have been a boon for Network Associates." Forbes **169**(3): 64.

Wodak, R. (2001). What CDA is about - a summary of its history, important concepts and its developments. Methods of critical discourse analysis. M. Meyer. London, SAGE: 1-13.

Zanini, M. (1999). "Middle Eastern Terrorism and Netwar." Studies in Conflict and Terrorism **22**(No. 3, Special Issue: Netwar Across the Spectrum of Conflict): 247-56.