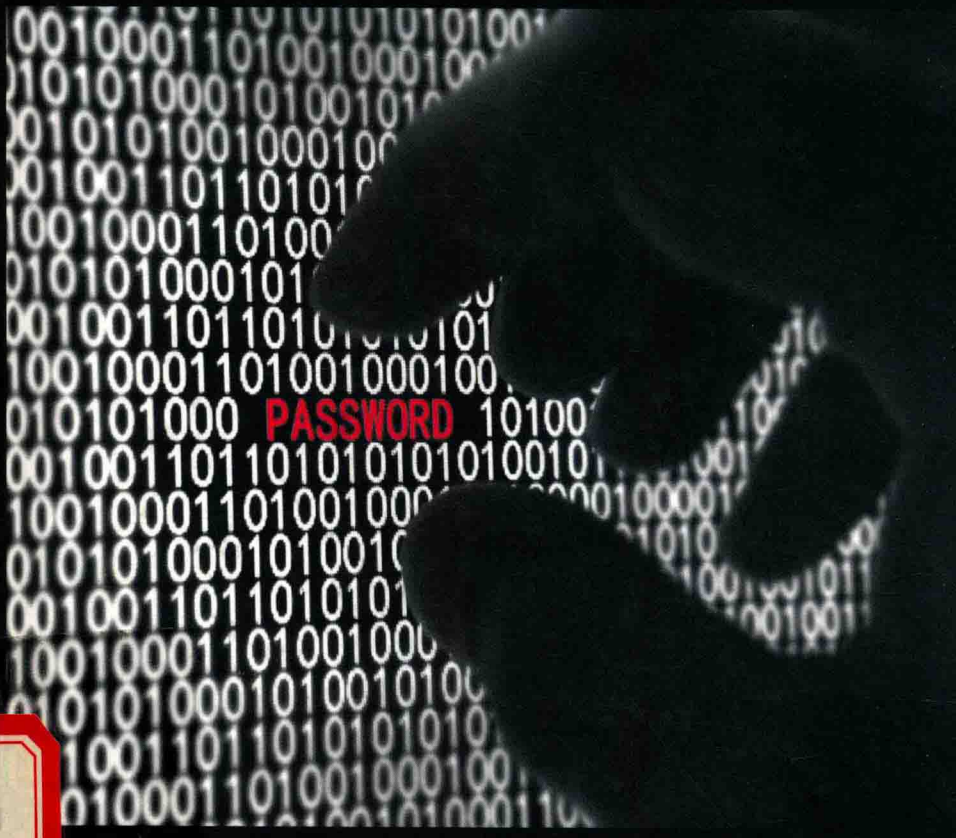
ASHGATE

Policing Cyber Hate, Cyber Threats and Cyber Terrorism



EDITED BY IMRAN AWAN AND BRIAN BLAKEMORE

Policing Cyber Hate, Cyber Threats and Cyber Terrorism

Edited By
IMRAN AWAN AND BRIAN BLAKEMORE
University of Glamorgan, UK

ASHGATE

POLICING CYBER HATE, CYBER THREATS AND CYBER TERRORISM

This work is dedicated to Sobia, Hiba, Shereen, Tasvir, and Liz, our beloved family members, who have supported us so well and forgiven us for the time we missed with our families whilst editing this text.

Imran and Brian

Notes on Contributors

Mr Imran Awan is a senior lecturer at the Centre for Police Sciences at the University of Glamorgan. He has taught on a variety of awards and modules such as International Police Duties and Law, Criminal Law and Criminal Justice, Terrorism, Law and Policy, and Violent Extremism and Terrorism. He has written numerous articles in the area of counter-terrorism, human rights and police powers and is the author of 'Terror in the Eye of the Beholder: The 'Spy Cam' Saga in Birmingham: Counter-Terrorism or Counter-productive?' published in *The Howard Journal of Criminal Justice.* In 2010, he was invited as a keynote speaker in the 'Combating Cyber terrorism, Online Crime and Law' series, by the School of Law at the University of Derby, [Available at: http://www.derby.ac.uk/news/combating-cyber-terrorism-and-online-crime; http://www.derby.ac.uk/news/laying-down-the-law] where he discussed counter-terrorism policy in relation to cyber terrorism. In March 2010 he was invited by the Office for Security and Counter-Terrorism to a Prevent Seminar held in London to discuss government policy on how to prevent violent extremism. He is currently involved in a research project that examines the impact of counter-terrorism legislation upon Muslim families in Cardiff. His areas of expertise include the study of extremism and radicalisation over the Internet, policing minority communities, the impact of counter-terrorist legislation upon Muslim families, policing in Pakistan and policing Pakistani gangs and culture. He is also a Fellow of the Higher Education Academy.

Mr Brian Blakemore is Head of the Police Sciences Division at the University of Glamorgan. Brian had previous experience on a wide range of academic awards with several academic management positions during his previous 26 years within this institution. Brian teaches on modules such as Science for Law Enforcement, Crime Investigation, Researching Police Practice and Researching Contemporary Issues. He has published on cognitive processes in investigation, Higher Education for police officers and professionalising the police force, the human rights aspects and investigative effectiveness of the national DNA database, and has co-edited three texts with Dr Colin Rogers on community and partnership working. Brian has also taught on several postgraduate programmes, often distance programmes, with the universities of Bradford, Bristol and Bath and also with Bristol Management centre. He is a vice chair of the Higher Education Forum for Learning and Development in Policing and represents this forum on the NPIA HE framework Steering Group.

Mr Geoff Coliandris is a former South Wales Police inspector, having served for 29 years in a range of posts including operational response, community safety and training. His police service included three periods of secondment to national police training bodies as well as project head/team leader roles at force level. He joined the university in 2006 as a part-time lecturer and has taught several modules on the Police Sciences degree award, including Police Duties and Law and Strategic Management in the Police Service. He has also taught on Foundation Studies Practical Skills for Police Officers and Foundation Degree (Leadership) modules. He has published (with Dr Colin Rogers) on police culture and leadership, partnerships and counter-terrorism and, most recently, police reform. He is also the author of a postgraduate diploma module on 'extremism' offered by the university as part of its Master's degree programme in Community and Partnerships.

Mr James Gravelle has previously worked for the University of Glamorgan as a consultant and research assistant (RA), and has carried out research on behalf of South Wales and Gwent Police Service. Research for the police included work on Tasking Demand Management Units (TDMUs), community intelligence, the use of volunteers and knowledge management. More recently, James now works within the division of Police Sciences as an associate lecturer and research officer. As an Associate of the Higher Education Academy, James has been involved in planning, writing and development of material within higher education on such areas as 'policing in the big society', 'knowledge management', 'policing in the financial crisis' 'the use of intelligence' and 'the impact of terrorism on policing'. As a Welsh-speaker, James also designs and delivers modules and material through the medium of Welsh. James has published many articles, papers and chapters in books over recent years aimed at both national and international audiences. James has given several radio and television interviews in relation to high profile police events and commenting on policing procedures and the impact of the economic situation of the delivery of policing services both in English and in Welsh. Being a member of many societies and groups such as the British Society of Criminology, and the European Society of Criminology, James also regularly attends and presents at national and European conferences on policing.

Dr Jane Prince is a Chartered Psychologist and Principal Lecturer in the School of Psychology at the University of Glamorgan where she is course tutor for two MSc awards; she has a particular research interest in identity, social identity and the ways in which individuals respond to threats and challenges to their identity positions. She has published on identity threats across the lifespan, identity issues in migration and social identity. Dr Prince's PhD research was on the challenges to identity experienced by policewomen; she has studied in Cardiff, London and Bordeaux and has worked in the UK, France and the Netherlands.

Mr Tim Read joined the University of Glamorgan in December 2007 and is now award leader for the Master's degree in Community and Partnerships. Previously he was Senior Research Consultant for Evidence-Led Solutions, a research consultancy working in the community safety field. Between 2001 and the end of 2005 he was a Senior Lecturer and Programme Leader for the Community Safety and Crime Prevention Master's degree course at the University of the West of England, Bristol. Prior to taking up the post at UWE he worked for the Research and Statistics Directorate of the Home Office for over 8 years, starting as a Research Officer, ending as a Principal Research Officer. He has extensive research and evaluation experience with the police and other criminal justice agencies and has published widely. He has just co-authored a book entitled *Policing and Young People* with Dr Colin Rogers.

Dr Colin Rogers is a former police inspector with South Wales Police with 30 years' service and joined the university full time in 2004, having taught as a part-time lecturer in criminology since 1997. His areas of expertise include community safety partnerships, situational crime prevention, problem oriented partnerships and also police governance and accountability. He is responsible for Research Study in the Division and is also responsible for developing postgraduate courses. The author of numerous articles on policing, he is also the author of four books, namely *Crime Reduction Partnerships* (2006), *Introduction to Police Work* (with Rhobert Lewis) (2007), *Leadership Skills in Policing* (2008), *Police Work: Principles and Practice*, (2011), (with Rob Lewis, Tim Read and Tim John) and has co-authored a series of three books with Brian Blakemore entitled *Problem Oriented Partnerships:* A Reader; (2009) *Crime Analysis and Evaluation:* A Reader; (2009) and *Community Safety: A Reader* (2009). He has just co-authored a book entitled *Policing and Young People with Tim Read.* Dr Rogers was awarded the title of Reader in Police Sciences in June 2010 in recognition for his research and scholarly activities.

Contents

Introduction

This text aims to bring together a diverse range of multidisciplinary ideas to explore the extent of cyber hate, cyber threat and cyber terrorism: studying its development, the present situation and look to the future of the forms and ability to police cyber hate, cyber threat and cyber terrorism. This text is designed to be a 'one stop shop' for all these aspects of cyber threat, cyber hate and cyber terrorism. The text will look at the psychology of potential cyber terrorists, the journey into cyber terrorism, the use of cyberspace by terrorists, the formation of cyber terrorist groups, the definitions of cyber terrorism will also be analysed and discussed, national legislation and international treaties and legislation will be critiqued in terms of effectiveness to combat the problems posed by cyber terrorism, the use of knowledge within the police and security services and how this may be marshalled to prevent and counter cyber terrorism. Also intelligence-led policing will be examined, the national strategies proposed by UK and other governments will be reviewed and their effectiveness examined. A final chapter will draw on all the preceding work to speculate on the future of policing cyber hate, cyber threats, and cyber terrorism. This is not an encyclopaedia but is more than an introduction and references and further reading are provided for the reader.

The text includes a study of the behaviour and motivations of cyber terrorists. The legal frameworks and legislation regarding cyber terrorism and its limitations in an international setting will be analysed. The public perceptions and understanding of cyber terrorism is also explored as is the policing and the threat of overreaction and working with communities to prevent development into terrorism. The main aim is to give a full understanding of the range of activities that form the spectrum of cyber threat, cyber hate to cyber terrorism; how such activity forms in our communities and what can be done to try to prevent individuals from becoming cyber terrorists.

There has been very little literature in this area as many academics have been trying to tackle what is cyber espionage and cyber attacks by state-sponsored governments so this book will provide a key insight into what the government regards as the main threat to UK security by making a contribution to this area of work. The text is multi-faceted as it covers the origins of cyber terrorism, how far it dates back and why we have missed a great opportunity in dealing with the problem. The book will give a policing rationale alongside specific e-crime units yet providing key details for policy readers as well as academics and students of this area.

The text may be considered to have two sections: the early chapters look at the background areas such as the concept of cyberspace and how it provides a platform for cyber hate, cyber threat and cyber terrorism, definitions of these terms

and analysis of the type of person likely to be recruited into activist groups and the methods used to recruit such individuals. Global networks of cyber criminals and cyber terrorists are creating new challenges for attorneys, judges, law enforcement agents, forensic examiners and corporate security professionals (Casey 2004:1) who are trying to find 'the balance between the need to maintain order online and the need to enforce the law' (Wakefield and Fleming 2009: 77). Sheldon and Wright state 'that cyber-security has become a national security issue' (2010: 10) that needs to be addressed. Ball and Webster (2003) argue that following the 9/11 attacks a massive expansion of security-surveillance capacities around the globe ensued. There was also an accompanying set of legislative powers such as the 'Patriot Act' in the USA which Roy (2004) describes as ushering in an automatic systematic of surveillance with the government using the powers to monitor phones, emails and computer use in general. While technology can aid prevention and detection of cyber crime, there have been notable design flaws, and aspects such as privacy and human rights issues need to be addressed. It can be appreciated that one piece of technology cannot be expected to be the 'silver bullet' of any specific form of cyber crime or cyber terrorism, and technology is double-edged enabling the criminal or terrorist as well as having a role in policing such activities. No security system can be considered impregnable to terrorist attacks such as a terrorist groups obtaining access to computers and hiding malicious software within them that then allows the computers to be controlled remotely (zombie computers). The necessary addresses to access such a set of zombie computers is called a botnet and again malicious software can be used to create such a botnet. The psychology relating to hate, terrorism and cyber hate and cyber terrorism is explored as well as an examination of the wider theories that relate to cyber crimes, such as social identity theory, social influence, the social identity model of de-individuation effects (side) and selective moral disengagement. The recruitment of individuals who are likely to become deployable agents ready to commit atrocities for the cause follows well-established patterns and processes and the use of the Internet enables activists to magnify the propaganda effect of their argument and to phish for suitable individuals. The amplification of the propaganda effect online is analysed using the terror management theory. Cyber hate is a phenomenon exhibiting multiple dimensions with hate-groups achieving their goals in four main ways: promoting ideology, promoting hatred of other racial or religious groups, exerting control over others and targeting opponents. The paradox of connectivity in relation to cyber hate is discussed.

The second section is concerned with policing this cyber activity and looks at the processes used to effectively combine data of many forms, from conversations on the street or networking sites, to police records of crime and criminals and biometric databases. The ability and desire to share of data and knowledge amongst the many agencies that need to work in partnership to prevent and catch cyber terrorists is examined. The level of need for more international cooperation and legislation to combat a global network of activists is explored. Finally we consider the overall position in relation to policing these cyber activities. However,

there are many questions on the best way to tackle cyber terrorism and ultimately whose responsibility it is to tackle it. The 'sheer volume of material generated, the global scope of the problem and the difficulty in applying laws to criminal activities across geographical boundaries' (Jewkes and Yar 2003:592), became apparent and an understanding surfaced that the 'scope, scale and structure of the Internet outstrips the capacity of any single enforcement or regulatory body' (Wall 2007:167). In response the UK government decided to restructure its cyber policing and formulate 'E-crime Strategy' in 2008, that aimed to coordinate local and international responses to cyber crimes through coordinated strategies and proactive responses. National and international strategies to deal with cyber terrorism need to be strengthened. Lenk (1997) comments that jurisdictional issues surrounding cyber crime go far beyond 'legal loopholes exposed within countries' (Slevin 2000:214), such as, 'double criminality', where a 'cyber criminal' cannot be extradited or charged for a crime committed in another country 'unless it constitutes a crime according to the laws of both the requesting and the requested states' (Shearer 1971:137). The scale and complexity of cyber crimes has compelled 'police partnerships with banks, telecommunication providers' (Broadhurst 2006:416) and with private security industries (PSIs) in order to tackle cyber crimes in an economic way. One possible model is the creation of private–public partnerships where private organisations would fund the monitoring of the Internet and breakdown 'raw' cyber crime data, and the public would pay for the arrest and prosecution of 'cyber criminals by their existing police service'. Even if strategies are agreed, implementation may fail if businesses or organisations are relied upon to implement them, if they are overwhelmed by costs or if it results in loss of convenience and reliability for the product, as noted by Burns and Weir (cited Jahankhani et al. 2008).Young (2009) suggests that 'the cost to industry and individuals of electronically assisted crime may have already far outstretched that of physical crime' (Eurim 2002:5) and as such the police must solely 'bear the brunt' of any cyber crime response because private organisations and ordinary citizens simply do not have the resources, time or money.

References

Ball, K. and Webster, F. (eds). 2003. *The Intensification of Surveillance: Crime, Warfare and Terrorism in the Information Age*. London: Pluto Press.

Broadhurst, R. 2006. 'Developments in the global law enforcement of cyber crime policing', *International Journal of Police Strategies and Management*, 29 (3), 408–33.

Jahankhani, H., Revett, R. and Palmer-Brown, D., 2008. *Global e-security: 4th International Conference, ICGeS 2008*. [e-book]. Germany: Springer. [Online]. Available at: http://books.google.co.uk/books?id=oeaTCy1Qaq4C&pg=PA40&dq=uk+card+fraud+capital+of+europe#v=onepage&q=uk%20card%20fraud%20capital %20of %20europe&f=false [accessed: 25 October 2010]. Casey, E. 2004. *Digital Evidence and Computer Crime*: *Forensic Science, Computers and the Internet*. San Diego: Academic Press.

EURIM. 2002. The European Information Society Group. *E-crime – A new opportunity of partnership briefing paper*, France: EURIM.

Jewkes, Y. and Yar, M. 2003. 'Policing Cybercrime: Emerging Trends and Future Challenges', in *Handbook of Policing*, edited by Newburn, T. Cullompton: Willan.

Lenk, K. 1997. 'The Challenge of Cyber Spatial Forms of Human Interaction to Territorial Governance and Policing', in *The Governance of Cyberspace*: *Politics, Technology and Global Restructuring*, edited by Loader, B. London: Routledge, 126–35.

Roy, A. 2004. *An Ordinary Person's Guide to Empire*. Cambridge MA: South End Press.

Shearer, I. 1971. *Extradition in International Law*. Manchester: Manchester University Press.

Sheldon, B. and Wright, P. 2010. *Policing and Technology*. Exeter: Learning Matters.

Slevin, J. 2000. *The Internet and Society*. London: Routledge.

Wakefield, A. and Fleming, J. 2009. *The Sage Dictionary of Policing*. London: Sage.

Wall, D. 2007. *Cybercrime*. Cambridge: Polity.

Young, T. 2009. *Foiling a Thoroughly Modern Bank Heist*. [Online]. Available at: http://news.cnet.com/8301–1009_3–10152246–83.htm [accessed: 17 October 2010].

Chapter 1
Cyberspace, Cyber Crime and Cyber Terrorism

Brian Blakemore

The terminology and concepts of cyberspace, cyber hate, cyber threats, cyber terrorism and policing need to be carefully defined. This chapter will examine how Cyberspace in particular lends itself to all these activities and assemble analogies from the wider field of cyber crime about which there is more information in the public domain. Initially the phrase cyber terrorism will be used in its broadest sense, recognising that it is the least well-defined of these terms. A full discussion of what cyber terrorism is and whether an activity is cyber hate, cyber threat or cyber terrorism is developed in Chapter 2 which will also include a more detailed analysis of cyber activities recognising that the computer can be both a weapon to be used and also the subject of a potential attack with examples such as possible attacks on critical national infrastructures such as gas, water, electricity and the use of digital steganography.

Cyberspace

Cyberspace may be considered as:

> a metaphor for describing the non-physical terrain created by computer systems. Online systems, for example, create a cyberspace within which people can communicate with one another (via e-mail), do research, or simply window shop. Like physical space, cyberspace contains objects (files, mail messages, graphics, etc.) and different modes of transportation and delivery. Unlike real space, though, exploring cyberspace does not require any physical movement other than pressing keys on a keyboard or moving a mouse … Some programs, particularly computer games, are designed to create a special cyberspace, one that resembles physical reality in some ways but defies it in others. In its extreme form, called virtual reality, users are presented with visual, auditory, and even tactile feedback that makes cyberspace feel real. (Webopedia nd)

Cyber refers to concepts of an organised movement and use of electronic data, and of control which is derived from manipulating such data. Space refers to the virtual place where two or more human activities interact. Cyberspace can be used

to describe simply the World Wide Web, the Internet as a whole and also to include all global media and communication channels. Sterling (1992) credits Barlow (1990) as the first to use the phrase cyberspace to refer to 'the present-day nexus of computer and telecommunications networks'.

This convergence of different media creates a world where all modes of communication and information are continually changing, not just the Information and Communication Technology (ICT) product used for communication but fundamentally 'changing the way we create, consume, learn and interact with each other' (Jenkins 2006). Current systems may be only at the 'end of the beginning' of this fundamental change as virtually all aspects of life, be they institutional activities such as business, government, art, journalism, health and education or recreational and social activities, are all increasingly being carried out in cyberspace across an ever-expanding and evolving network of information and converging communication technology devices. ICT is defined by Schuchart (2003:np) as:

> an umbrella term that includes any communication device or application, encompassing: radio, television, cellular phones, computer and network hardware and software, satellite systems and so on, as well as the various services and applications associated with them, such as videoconferencing and distance learning.

The Internet forms the backbone of cyberspace and is a global network of individual computer systems owned by businesses, governments and other public bodies and even individuals. The World Wide Web, which was launched in late 1990, operates within the Internet and is a network of linked multimedia information (web pages) available to all (universality). The technical standards are open and royalty-free and allow anyone to create applications without requiring formal permission or sanction. This is accomplished using common naming (address) and production protocols (URL (uniform resource locator) and HTTP (hypertext transfer protocol)).

The pace of technological change is rapid and accelerating. 'On the 15th June 2009, 20 hours of new content were posted on YouTube every minute, 494 exabytes [a billion gigabytes] of information were transferred seamlessly across the globe, over 2.6 billion mobile phone minutes were exchanged across Europe and millions of enquiries were made using a Google algorithm' (Lord Carter, cited in Sheldon and Wright 2010:165). This convergence coupled with the ubiquitous low cost and ease of operation of future ICT systems, suggests that cyberspace will become the place where all our senses coincide with all possibilities of thought and action. Weiser (1991) coined the term 'ubiquitous computing' in 1988 referring to a future time when devices and systems would be so numerous and integrated into our lives that technology becomes the media through which people live. This time is nearly upon us and that the final boundary between online life and real life is already ill-defined.

Burns and Weir (cited in Jahankhani et al. 2008:45) propose that 'Security is a balance between confidentiality, authentication and integrity versus convenience, cost and reliability'. Such factors must be taken into account in the development of new anti cyber crime interventions and especially for technology to support such interventions. This view is supported by Everett (2006) who stated that '... perfect security is not economically viable even if practically achievable'. Security systems within cyberspace require continuous innovation in order to match the rapid pace of general technological advancement in cyberspace and the new potential cyber crime opportunities such development produces. It has been asserted that '... design flaws and errors are normally the main cause of security holes that are explored by attackers' (Khan and Mustafa 2009:10). Generally technological developments are far from perfect; for example, Chip and PIN has not eliminated all plastic card fraud. If there are loopholes, cyber criminals and cyber terrorists will seek these and exploit them to their advantage. Even when advances are made, the length of time taken to roll them out across the world may allow for cyber criminals and cyber terrorists to continue operating and initiate ways of countering these advances as they become widespread. With the government and mass media raising awareness of new breakthroughs, cyber criminals and cyber terrorists receive prior warning of the need to develop new ways to penetrate and attack the new technology.

There are a number of crucial factors affecting any new ICT or online security systems success; for example, do they depend upon implementation by another organisation? Kovacich (2007:156) stated, 'We should never consider any high technology device, any controls, or any portion of any anti fraud program to be able to stop 100 per cent of all fraud threat agents or to thwart all fraud schemes, all we can ever expect is the levels of risk to be made as low as possible'. In support of this statement, Levi and Handley (2002:16) announced, 'Unless a completely secure payment system is devised, then there will inevitably be some risk, and greater use will normally provide more opportunities for fraud' and 'With sophisticated technical systems, the weakest link is often human error' (ibid:20). Both authors are critical of the expectations often associated with new technology. Many ICT users' understanding of security issues is lagging behind technological developments; for example according to one study, 56 per cent of Internet users did not understand what a 'cookie' was and how it held useable information about the Internet user's activities (Pew Internet and American Life project 2000:3). However, if all the stakeholders work together cyber crime can be reduced. The UK Card association report a 17 per cent reduction in reported crime involving credit cards during 2010. This is attributed to a combination of efforts amongst the card industry, banks and consumers (UKCA 2011) and Financial Fraud Action UK (2011:1) report reduced levels of some cyber crime in 2010: 'Online banking fraud losses totalled £46.7 million in 2010 – a 29% fall from the 2009 figure', demonstrating that using existing security measures can reduce the rate of these crimes but not prevent them. If this is also the case for cyber terrorism then such

terrorist acts will continue so long as there is a political, religious or ideological will to commit such activities.

There is a technological arms race between cyber criminals and those policing cyberspace; the race is one of technological leapfrog with each side trying to make an advantage and capitalise on it during a brief period of technological supremacy. The time frame during which harmful activities can occur in cyberspace is much shorter than in a non-ICT system but the scope for gain or damage is significantly greater. Wall (2007) describes the current situation as the third generation of cyber crimes utilising networked technologies that are converging with other technologies.

One example of such technological leapfrogging is the discovery of a tailored computer attack in a process control system. Generally, malicious software programs that attack systems or steals information from systems are known as worms that spread across networks by finding and using security flaws or viruses that inhabit static files and require the user to unwittingly assist with their spread. Specifically the 'Stuxnet' worm was discovered in Sieman's propriety software systems that are used to control and monitor the performance of industrial processes. The worm rewrote the computer controllers in the system, and concealed these changes. Stuxnet is estimated to have infected 100,000 host computers and although this worm has been found worldwide, 60 per cent of the infections have been linked to Sieman's systems in Iran (TCE 2010a), suggesting a focused cyber state-sponsored attack that is undoubtedly designed to slow the development of Iran's nuclear capability: this may be an example of a cyber threat or even cyber warfare. These issues are discussed in greater depth in Chapter 2. Iran has confirmed that the worm caused problems at its enrichment plant in Natanz (TCE 2010b). The infection spread from five industrial domains that have operations in Iran and that were linked to the Natanz uranium production facility to impede this site's operation (TCE 2011). A spokesperson from the security firm Kaspersky described Stuxnet as 'a working and fearsome prototype of a cyber-weapon that will lead to the creation of a new arms race' (BBC News 2010b).

Other cyber attacks include the following: in 2007, Estonia was the subject of a series of cyber attacks which crippled the Internet across the country; Operation Aurora attacks on Google in China in January 2010 penetrating this ICT company's protective software, targeting information on human rights activists; and the 'Night Dragon', a series of ongoing attacks which are coordinated attempts to penetrate at least a dozen multinational oil, gas and energy companies that began in November 2009. These attacks exploited Microsoft's operating systems despite the security systems installed by these organisations (TCE 2011). The National Security Review (HM Government 2010) rated cyber attacks as a tier one risk to the UK's security – the highest possible level of threat. There is no completely secure Internet system (TCE 2011) which raises the risk of successful cyber attacks following the introduction of increasingly complex Internet-based systems such as Cloud Computing.

Cloud computing replaces the storing of bought software on individual computers with the rental of such software on servers and accessing the software via the Internet. Organisations can expand processing power by adding more servers. There are already both public and private clouds systems in operation (Greenaway 2010). Cloud computing had a market worth $47 billion in 2008 and will be ubiquitous within 3 years according to Microsoft, with 20 per cent of email using cloud computing by 2012 (Payton 2010). This will allow organisations to save money on internal ICT services and to spread costs of new software over a longer period via rental rather than purchasing licence agreements. However, this will fundamentally shift the onus for security to the Internet-based provider. The advocates of cloud computing argue that such providers will have the resources, that is, finance and technical expertise, to provide more enhanced security than the present system which depends very much upon individual organisations perceptions of risks, technical ability, expertise and outlook. The breaching of Sony's PC games site (Goodin 2011) demonstrates that very large organisations that have invested considerable resources into their network security cannot be considered 100 per cent secure and that the personal details of its 77 million customers may have been accessed. Certainly Facebook, a cloud-based system, has become a part of daily life for many people in modern society. The US, Japanese and UK governments are all launching cloud applications (Greenaway 2010) and need to come to terms with some processing of their data taking place outside their national boundaries. Governments will be concerned with access to sensitive data and will use encryption, access and storage security measures within their risk assessments to decide precisely what can be located on a cloud application (Greenaway 2010).

Encryption technology, such as the digital certificates used to secure payment transactions using Paypal, allows users to protect their files from being opened by others but this tool can be employed by cyber criminals and cyber terrorists to keep their own material secure from police and security monitoring activities. Oliver Drage was imprisoned for 4 months for refusing to reveal his 50-character encryption key to Lancashire police who were investigating child exploitation. Seventeen months after seizing his computer they had still not cracked his code (Radenedge 2010). With the emails sent by Rajib Karim, a convicted terrorist, it took a team of code-breakers nine months to crack the codes he used (Twomey 2011). Encryption can use several layers of data and can include more than keyboard characters by using graphics and photographs to compose the key or code (Radenedge 2010). Further discussion of encryption and digital steganography follows in Chapter 2. Government legislation such as in the USA has required providers to design and provide a 'backdoor' into encrypted programmes so that law enforcement agencies can more easily read messages but this also allows for the possibility of hackers or terrorists finding and accessing this 'backdoor'. The legislative approaches to dealing with cyber terrorism are discussed more fully in Chapter 6.