Computer Hacking and Cyber Terrorism: The real threats in the new Millennium?

S.M.Furnell[†] and M.J.Warren[‡]

[†] Network Research Group, School of Electronic, Communication and Electrical Engineering, University of Plymouth, Plymouth, UK.
[‡] School of Computing and Mathematics, Deakin University, Geelong, Victoria, Australia.

e-mail: sfurnell@plymouth.ac.uk, m.warren@deakin.edu.au

Abstract

As the new millennium approaches, we are living in a society that is increasingly dependent upon information technology. However, whilst technology can deliver a number of benefits, it also introduces new vulnerabilities that can be exploited by persons with the necessary technical skills. Hackers represent a well-known threat in this respect and are responsible for a significant degree of disruption and damage to information systems. However, they are not the only criminal element that has to be taken into consideration. Evidence suggests that technology is increasingly seen as potential tool for terrorist organisations. This is leading to the emergence of a new threat in the form of 'cyber terrorists', who attack technological infrastructures such as the Internet in order to help further their cause. The paper discusses the problems posed by these groups and considers the nature of the responses necessary to preserve the future security of our society.

Keywords

Cyber Terrorism, Hackers, Information Warfare, Internet, Security.

Introduction

As we approach the new millennium, much has been made of the so-called 'Year 2000 Problem' or 'Millennium Bug' [1]. Concern over the problem is no doubt justified in many cases and, consequently, demands that appropriate action be taken to avoid (at the very least) significant disruption to everyday services. However, in a wider sense, the millennium bug panic should also act as our 'wake-up call' to a more general concern, namely modern society's overall dependence upon information technology and communications systems. This statement is in no way intended to promote a Luddite perspective and suggest that IT is a negative influence, but it must be recognised that it brings new threats to the society that it is, in other ways, benefiting.

From the perspective of someone wishing to cause damage, there is now the capability to undermine and disable a society without a single shot being fired or missile being launched. To see the truth of this, it is only necessary to consider how many essential areas of modern society are now so significantly dependent upon technology that its unavailability could be catastrophic, for example:

- healthcare;
- banking / finance;
- manufacturing;
- transportation;
- government.

Undermine the technology infrastructure and consider the impact: manufacturing would cease, access to money would be frozen and people in need of care or support would not receive it. The new industries of the next millennium, such as electronic commerce, could be the first victims of this new style of problem.

All of the above effects could conceivably occur as a result of an accidental incident or a lack of foresight (e.g. in the same way as the Millennium Bug issue came about). However, this paper sets out to consider the potentially more alarming scenario in which technology infrastructures or services are targeted deliberately. The protagonists in such a scenario could conceivably come from many backgrounds. For the purposes of discussion, however, the paper will consider them under the general categories of 'hackers' and 'cyber terrorists'.

New Threats of the Information Age

The aforementioned Millennium Bug represents a clear threat to the information society and has the potential to cause significant damage if organisations are not properly prepared. However, it is a problem related to a specific point in time and it is likely that the issue will have been safely forgotten by the majority of organisations in a few months after 1 January 2000. The issues of computer hackers and cyber terrorists can be considered to represent longer-term threats to the Information Society. This section examines the nature of the problems and how they are developing.

Hackers

The term 'hacker' was originally used in computing circles to refer to individuals who had a low-level familiarity with the operation of technology and were capable of devising technically elegant software solutions [2]. However, the usage of the term has changed over the years and is now generally accepted as referring to persons who deliberately gain (or attempt to gain) unauthorised access to computer systems.

Hackers are by no means a new threat and have routinely featured in news stories during the last two decades. Indeed, they have become the traditional 'target' of the media, with the

standard approach being to present the image of either a "teenage whizzkid" or an insidious threat. In reality, it can be argued that there are different degrees of the problem. Some hackers are malicious, whilst others are merely naïve and, hence, do not appreciate that their activities may be doing any real harm. Furthermore, when viewed as a general population, hackers may be seen to have numerous motivations for their actions (including financial gain, revenge, ideology or just plain mischief making). However, in many cases it can be argued that this is immaterial as, no matter what the reason, the end result is some form of adverse impact upon another party.

Table 1 illustrates the extent of the hacking problem, based upon figures taken from a series of surveys conducted by the UK Audit Commission [3,4,5]. These surveys consider the general problem of computer abuse, encompassing various types of incident (including hacking, viruses, fraud, sabotage and theft) across a number of industries / sectors (including government, healthcare, banking, retail and education). The table indicates the consequences of the incidents in terms of financial losses (which may have occurred directly or indirectly as a result of the incidents). However, it is likely that other, less measurable consequences may also have occurred as a result (e.g. disruption to operations, breaches of personal privacy or commercial confidentiality etc.).

	1987	**1990**	**1994**	**1998**
Total abuse incidents reported	118	180	537	510
No. hacking incidents	35	26	15	56
Hacking as % of total	30%	14%	3%	11%
Resulting loss (£)	£100	£31,500	£16,220	£360,860

Table 1 : Reported incidents of computer hacking

As an aside, it is worth noting that the significant increases in the 'total incidents' figures in the 1994 and 1998 surveys are largely accounted for by the widespread emergence of the virus problem. It should also be noted that these figures only refer to the *reported* incidents – it is frequently speculated that the true figures may be much higher than this, but organisations are choosing to remain silent in order to avoid adverse publicity and the like [6].

The list below highlights a small variety of the activities that hackers have been known to engage in. In many cases there have been reported incidents of hackers not only gaining unauthorised access (i.e. potentially breaching confidentiality), but also altering data or service provision (i.e. affecting integrity and/or availability):

- Modfication of medical records [4];
- Breach of Military systems [7];
- Monitoring and alteration of telecommunications services [8].

As can be seen, breaches in all of the above categories of system offer significant opportunities to inflict damage (to both organisations and individuals) and, therefore, illustrate the nature of the hacker threat. Incidents such as those referenced indicate that many of our systems are vulnerable and that if someone has the inclination, and is willing to put in the effort, then existing security can often be breached. Furthermore, the evidence suggests that it is possible to breach systems that we would instinctively expect to be more secure (e.g. military sites). The fact that such attacks are successful leaves systems vulnerable to more insidious threats than straightforward hacking, in which information systems become the target in a more sinister way.

Cyber Terrorists

Recent years have witnessed the widespread use of information technology by terrorist-type organisations. This has led to the emergence of a new class of threat, which has been termed Cyber Terrorism. This can be viewed as distinct from 'traditional' terrorism since physical terror does not occur and efforts are instead focused upon attacking information systems / resources.

When viewed from the perspective of skills and techniques, there is little to distinguish cyber terrorists from the general classification of hackers. Both groups require and utilise an arsenal of techniques in order to breach the security of target systems. From a motivational perspective, however, cyber terrorists are clearly different, operating with a specific political or ideological agenda to support their actions. This in turn may result in more focused / determined efforts to achieve their objectives and more considered selection of suitable targets for attack. However, the difference does not necessarily end there and other factors should be considered. Firstly, the fact that cyber terrorists are part of an organised group could mean that they have funding available to support their activities. This in turn would mean that individual hackers could be hired to carry out attacks on behalf of a terrorist organisation (effectively sub-contracting the necessary technical expertise). In this situation, the hackers themselves may not believe in the terrorist's 'cause', but will undertake the work for financial gain.

Established terrorist groups (or related organisations) are currently using the Internet for a number of purposes, as described below.

- **Propaganda/Publicity**
  Terrorist/resistance groups have traditionally had difficulty in relaying their political messages to the general public without being censored. However, they can now use the Internet for this purpose. Examples of where this is already the case include the Irish Republican Information Service (http://joyce.iol.ie/~saoirse/) and the Zapatista Movement (http://www.ezln.org/).

- **Fundraising**

Some terrorist/resistance groups linked to political parties are now using the Internet for funding raising purposes. In the future this may mean that smaller terrorist/resistance groups may be able to receive the majority of their funding through credit card donations.

- **Information Dissemination**
  It is also possible that groups may publish sensitive information about a particular country. For example, Sinn Fein supporters at the University of Texas made details about British Army establishments within Northern Ireland publicly available on the Internet [9]. In addition, information is available about engaging in terrorist activities. For example, the 'Terrorist Handbook' [10] instructs beginners how to make explosives and weapons and is widely referenced and available on the Internet.

- **Secure Communications**
  Terrorist use of more advanced encryption methods [11] and improved anonymous electronic re-mailers will result in a command system that is difficult to break and allows for the control of groups anywhere in the world. This causes a problem for the security services, as it means that they will have to spend more time and resources on trying to decrypt electronic messages.

Whilst all of the above might give cause for concern, they merely illustrate how existing activities may be simplified via new technology. The real threat in the 'cyber' context is when the Internet (or the more general technology infrastructure) becomes the medium in which a terrorist-type attack is conducted. In this sense, it is somewhat ironic that the Internet (which was originally conceived as a means of ensuring continued communications in the event of a nuclear war destroying the conventional telecommunications infrastructure) should now itself represent a medium through which widespread damage can be caused to the new information society.

It is possible to view technology as some kind of "great equaliser" between major countries / governments and smaller groups. This is a battlefield where success relies upon intellectual skills and software creativity as opposed to sheer volume and physical resources. In short, the individuals or small groups may, in theory, have as much chance of succeeding as a superpower.

To see the potential for damage, you only have to look at the results of actions from individuals who have acted *without* a war motive and *without* government / official backing. Consider the impact that computer hacking and virus incidents have had upon businesses in recent years. In purely financial terms, the impact can be seen to be significant, as shown by the earlier figures from table 1. A separate survey, published by the UK National Computing Centre in 1996, revealed that the average cost of a hacking incident was around £14,460, whilst viruses typically resulted in a financial cost of £4,190 [12]. Imagine what would be possible if a more determined/concentrated effort was made to co-ordinate these attacks.

The most significant threats come from the integrity and availability aspects. Security breaches in these respects have the potential to do the most direct damage (e.g. by making

systems unavailable or having them operate on the basis of incorrect data). Breaches of confidentiality could, however, have an indirect value in a terrorism or warfare context. They could, for example, be used to provide a distraction or destabilising effect to an established power (e.g. consider the effect of the media's preoccupation with the Clinton / Lewinsky affair and the extent to which this served to distract public attention from other national or world events). The potential for direct damage, however, comes from other activities. The term Information Warfare has been used to describe the ways in which terrorist organisations could use technology to attack the IT infrastructure of a country or a particular company [13]. Common scenarios include Denial of Service and Direct Attacks, as described below.

A denial-of-service attack results when access to a computer or network resource is intentionally blocked or degraded as a result of malicious action taken by another user. These attacks do not necessarily cause direct or permanent damage to data, but they intentionally compromise the availability of the resources [14]. This type of attack tends to affect the availability of computer systems for legitimate usage and the form of the activity can include methods such as e-mail bombs - sending thousands of emails to a particular computer system until that system crashes. The software required to carry out denial of service attacks is widely available on the Internet. The first recorded cyber terrorist denial of service attack was carried out the by Tamil Tigers against Sri Lankan embassies around the world [15].

A direct attack would take the form of hacking into a computer system and rewriting or stealing information. For example, the Portuguese hacker group PHAIT (Portuguese Hackers Against Indonesian Tyranny), rewrote Indonesian government and commercial web sites in order to protest about East Timor, as illustrated in figure 1. Since 1997 this group has hacked and defaced (according to their sources): 20 government systems; 14 commercial systems; one academic system and another nine minor government systems. Their campaign is still on-going against the government of Indonesia.

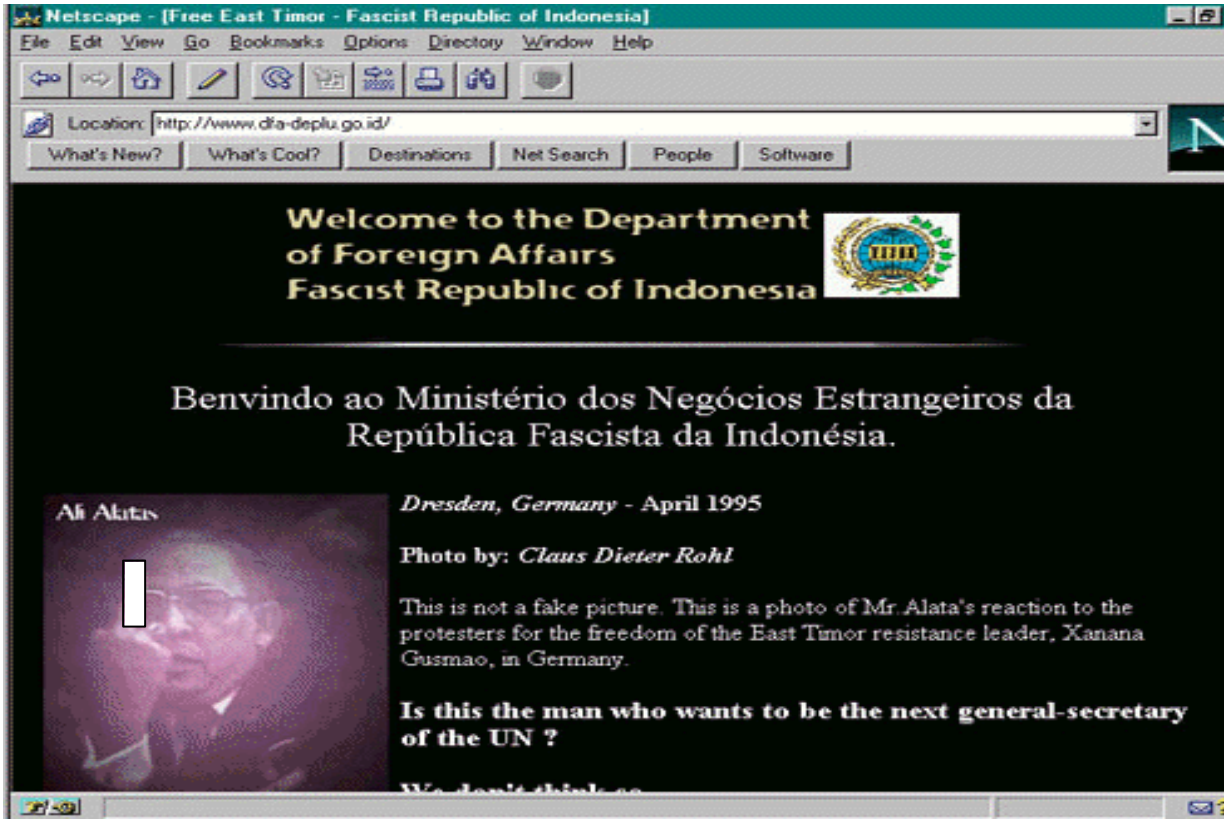

Figure 1: Aftermath after a Terrorist/Resistance Group Hacker Attack

An indication of the scale of the problem can be obtained by considering particular high-profile targets. For example, the US Department of Defense (DoD) claims that its WWW sites experience around 60 attacks each week. In 1995 alone, the DoD claimed to have been attacked 250,000 times [16]. The nature of these 'attacks' may well vary, and some will certainly be less significant than others, but the overall figure nevertheless illustrates the interest that unauthorised parties have taken in the military systems. As an aside, the US military has now begun to rethink its attitude towards the use of the Internet and has undertaken a review of the material that is published on its web sites in order to prevent sensitive information from being made available inadvertently [17].

Another observation is that cyber attacks offer the capability for terrorist activities with wider-reaching impacts. With traditional terrorist activities, such as bombings, the impacts are isolated within specific physical locations and communities. In this context, the wider populous act only as observers and are not directly affected by the actions. Furthermore, acts of violence are not necessarily the most effective ways of making a political or ideological point – the media / public attention is more likely to focus upon the destruction of property and / or loss of life than whatever 'cause' the activity was intended to promote. The ability of cyber terrorism activities to affect a wider population may give the groups involved greater leverage in terms of achieving their objectives, whilst at the same time ensuring that no immediate long-term damage is caused which could cloud the issue. For example, in a denial of service scenario, if the threatened party was to accede to the terrorist

demands, then the situation could (ostensibly at least) be returned to that which existed prior to the attack (i.e. with service resumed). This is not the case in a 'physical' incident when death or destruction have occurred.

A final point to note is that cyber terrorist activity could also be used in conjunction with or to support more traditional attacks. For example, hacking techniques could be employed to obtain intelligence information from systems, which could then be used as the basis for a physical attack.

Methods of Response

Having considered the nature of the threats, it is appropriate to consider what is needed to address them and the extent to which appropriate action is already being taken.

The hacker problem is now widely recognised and many countries already have some form of associated legislation. An example of this is the Computer Misuse Act in the United Kingdom, which specifies offences ranging from unauthorised system access to unauthorised modifications to programs or data [18]. However, the mere presence of legislation is not sufficient – law enforcement and the judiciary must be suitably prepared to administer it. Some previously documented cases of hacker / computer abuse investigations have indicated that this may not be the case and the criminals often have a significant upper hand in terms of their understanding of technology. A good example of this is provided by Stoll [19] in his recounting of the experiences of law enforcement whilst tracking the so-called 'wily hacker'.

It is difficult to predict precisely how terrorists groups may use the Internet in the future. However, it is considered that cyber terrorism will become more attractive to terrorist groups. The principal reasons for this are as follows [20]:

- the risk of capture is reduced since attacks can occur remotely;
- it is possible to inflict grave financial damage without any loss of life;
- the expertise for these attacks can be hired;
- a successful attack would result in world wide publicity and failure would go unnoticed;
- terrorist groups can attract supporters from all over the world;
- they can use the Internet as a method of generating funds for their cause world wide;
- the Internet offers the ideal propaganda tool for a terrorist group, one that operates on a global basis and that individual governments cannot control or censor;
- the capability to mount an attack can be developed both quickly and cheaply.

The seriousness with which the issue is taken can be illustrated by recent activities by national governments. In the United States, for example, concern over IT related threats has led to the establishment of the National Infrastructure Protection Centre (NIPC). This is a $64 million facility, employing some 500 staff across the country, with representatives taken from existing agencies such as the Secret Service, the CIA, NASA, the National Security

Agency, the Department of Defense and several others. The role of NIPC is to "detect, deter, assess, warn of, respond to, and investigate computer intrusions and unlawful acts" that threaten or target US critical infrastructures such as telecommunications, energy, banking and finance, water systems, government operations and emergency services [21].

Whilst the threats are undoubtedly serious, we must be careful to ensure that our methods of response are not taken too far. Without appropriate control, it is possible that measures could be introduced that are harmful to society in a different way. For example, the complete regulation or monitoring of our use of IT systems could lead to the emergence (some would say extension) of a "surveillance society" in which technology is used to erode individual rights and freedoms in the name of the wider public good [22].

It can already be seen that the activities of both hackers and cyber terrorists ultimately have the effect of restricting freedoms for the rest of us. For example, despite some concessions, the United States continues to maintain a relatively restrictive policy on the use of cryptographic technologies. One of the stated reasons for control is to prevent unregulated use of strong encryption techniques by terrorist organisations [23].

Conclusion

Whether we like it or not, modern society has a significant (and increasing) dependence upon information technology. This paper has sought to suggest that, as a result of this, we face a number of immediate and long-term threats that need to be recognised in order for protective action to be taken. This discussion has focused upon the particular threats represented by hackers and cyber terrorists.

In the case of hackers we can, to some extent, take comfort from the fact that a significant proportion of them are not engaging in their activities for a malicious purposes. This is good news because, in many ways, the hacker threat is likely to be more difficult to police than that of cyber terrorism. The reason for this is that the number of casual hackers far exceeds the number of cyber terrorist organisations and their targets may be much less predictable. At the same time, however, the impact of any individual attack is likely to be less severe.

Cyber terrorists operate with a political agenda. This motivation (which could often be more accurately described as fanaticism) will mean these types of attacks will be more specifically targeted and aimed at more critical systems. This collective action would do more harm than the action of a single hacker. There is also the issue of funding, since terrorist groups could have substantial funds available, this means that they could easily employ hackers to act on their behalf.

In a way, the existence of hackers and cyber terrorists lends credibility to the concept of a cyberspace information society. Any true society will always include elements that many of its other members would consider to be undesirable. However, it also indicates that the information society is unlikely to be the Utopian ideal that many have predicted. Technology

will not solve all of the problems from our current society – many will simply re-emerge in different forms.

References

[1] Ulrich, W.M. and Hayes, I.S. 1997. *The Year 2000 Software Crisis*, Yourdon Press Computing Series, Prentice Hall, ISBN 0-13-655664-7.

[2] Levy, S. 1984. *Hackers : Heroes of the computer revolution*. Anchor Press / Doubleday.

[3] Audit Commission. 1990. *Survey of Computer Fraud & Abuse*.

[4] Audit Commission. 1994. *Opportunity Makes a Thief: An Analysis of Computer Abuse*, National Report, London, HMSO.

[5] Audit Commission. 1998. *Ghost in the Machine – An Analysis of IT Fraud and Abuse*. Audit Commission Publications, UK. February 1998. ISBN 1-86240-056-3.

[6] Nycum, S.H. and Parker, D.B. 1990. "Prosecutorial experience with state computer crime laws in the United States", in *Security and Protection in Information Systems*, A.Grissonnanche (Ed.), Elsevier Science Publishers B.V., North-Holland: 307-319.

[7] Niccolai, J. 1998. "Israeli Arrested for Hacking U.S. Military Computers". IDG News Service, March 19, 1998. See http://www.infowar.com/.

[8] Littman, J. 1997. *The Watchman – The Twisted Life and Crimes of Serial Hacker Kevin Poulsen*. Little, Brown & Company Limited. ISBN 0-316-52857-9.

[9] Tendler, S. 1996. "Ulster security details posed on the Internet", The Times, 25 March 1996, UK.

[10] Anonymous. 1994. *The Terrorist's Handbook*. Available on Internet / WWW.

[11] Malik, I. 1996. *Computer Hacking: detection and protection*. Sigma Press, UK, ISBN 1-85058-538-5.

[12] NCC. 1996. *The Information Security Breaches Survey 1996*. National Computing Centre, Oxford Road, Manchester, UK.

[13] Schwartau, W. 1994. *Information Warfare: Chaos on the Electronic Superhighway*. Thunder's Mouth Press, New York.

[14] Howard, J. 1997. An Analysis Of Security Incidents On The Internet. PhD thesis, Carnegie Mellon University, USA.

[15] Associated Press. 1998. "First cyber terrorist action reported", May 6th, USA.

[16] McKay, N. 1998. "Cyber Terror Arsenal Grows", Wired News, 16 October 1998. http://www.wired.com/news.

[17] Booth, N. 1998. "Pentagon gets tough in war of the Web", *The Times*, Interface Supplement, 7 October 1998: 2.

[18] HMSO. 1990. *Computer Misuse Act 1990*. Her Majesty's Stationary Office, UK. ISBN 0-10-541890-0.

[19] Stoll, C. 1991. *The Cuckoo's Egg*. Pan Books Ltd, London, UK. ISBN 0-330-31742-3.

[20] Warren, M. 1998. "Cyber Terrorism", Proceedings of SEC-98 - IFIP World Congress, Budapest, Hungary, August 1998.

[21] NIPC. 1998. Mission Statement, National Infrastructure Protection Centre. http://www.fbi.gov/nipc/nipc.htm

[22] Davies, S. 1996. Big Brother – Britain's web of surveillance and the new technological order. Pan Book Ltd, London. ISBN 0-330-34931-7.

[23] FBI. 1998. *Encryption: Impact on law Enforcement*. Information Resources Division, Federal Bureau of Investigation, Virginia, US. 8 July 1998.