CYBER-TERRORISM – THE POLITICAL EVOLUTION OF THE COMPUTER HACKER

M.J.Warren[†] and S.M.Furnell[‡]

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

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

Abstract

The computer hacker already represents a well-known threat in the context of the global information society and is held responsible for a significant degree of disruption and damage to information systems. However, evidence suggests that hacking skills are now being applied for distinctly political purposes. The consequence is that information technology is increasingly seen as potential tool for terrorist organisations. This is leading to the emergence 'cyber terrorists', who attack technological infrastructures such as the Internet in order to help further their cause. The paper considers the potential problems, presents some evidence to highlight known examples (particularly in the context of the Balkans crisis) and discusses the responses necessary to preserve the future security of our society.

Keywords
Cyber Terrorism, Hackers, Internet, Security.

1) Introduction

Many aspects of our modern society now have either a direct or implicit dependence upon information technology (IT). As such, a compromise of the availability or integrity in relation to these systems (which may encompass such diverse domains as banking, government, healthcare and law enforcement) could have dramatic consequences from a societal perspective.

In many modern business environments, even the short-term, temporary interruption of Internet / e-mail connectivity can have a significantly disruptive effect, forcing people to revert to other forms of communication that are now viewed as less convenient. Imagine, then, the effect if the denial of service was over the longer term and also affected the IT infrastructure in general. Many governments are now coming to this realisation.

This paper sets out to consider the scenario in which technology infrastructures or services are targeted deliberately, examining the issue in relation to two categories of computer abuser: 'hackers' and 'cyber terrorists'.

2) The Computer Hacker

The definition of the 'computer hacker' has been the subject of much debate in computing circles. Caelli et al (1989) provide two definitions of the term:

1. In programming, a computing enthusiast. The term is normally applied to people who take a delight in experimenting with system hardware (the electronics), software (computer programs) and communication systems (telephone lines, in most cases).

2. In data (information) security, an unauthorised user who tries to gain entry into a computer, or computer network, by defeating the computers access (and/or security) controls.

In mass media terms, the latter interpretation is by far the more common (although persons belonging to the former category of hacker would seek to more accurately define the latter group, particularly those with a malicious intent, as 'crackers').

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 (Audit Commission 1990, 1994, 1998). 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.).

	1990	1994	1998
Total abuse incidents reported	180	537	510
No. hacking incidents	26	15	56
Hacking as % of total	14%	3%	11%
Resulting loss (£)	£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 (Nycum and Parker 1990).

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):

- Modification of medical records (Audit Commission 1994);
- Breach of Military systems (Niccolai 1998);

- Monitoring and alteration of telecommunications services (Littman 1997).

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.

3) Enter the Cyber Terrorist

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 (Tendler 1996).

- *Secure Communications*
  Terrorist use of more advanced encryption methods (Malik 1996) 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 (NCC 1996). 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 last year's media preoccupation with the Clinton / Lewinsky affair and the extent to which it 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 (Schwartau 1994). 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 (Howard 1997). 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 (Associated Press 1998).

A direct attack would take the form of hacking into a computer system and rewriting or stealing information. Examples of this are given in the next section, in relation to the crisis in the Balkans.

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 (McKay 1998). 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 (Booth 1998).

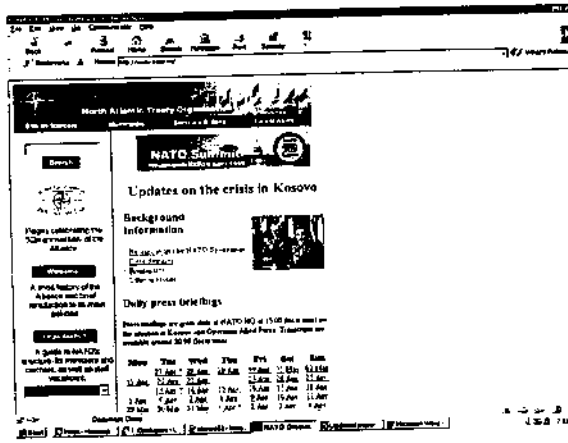
Another observation is that cyber attacks offer the capability for terrorist activities with wider-reaching impacts. With traditional terrorist activities, such as bombings, the impacts are isolated within specific physical locations and communities. In this context, the wider populous act only as observers 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 has 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.

4) The Balkans – cyber warfare in action

The recent escalation of violence in the Balkans has also resulted in the development of a new front to the war – the cyber front. Both sides have used the Internet as a means of putting their point of view forward. Both sides in the conflict are using the Internet to report the news from their own perspective, as illustrated in figures 1 and 2.

Figure 1: Official NATO web-Site



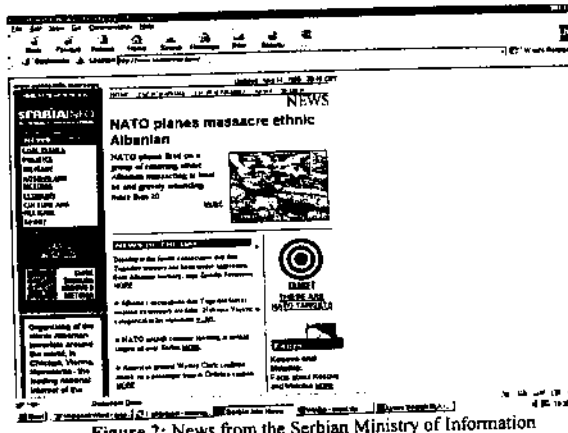


Figure 2: News from the Serbian Ministry of Information

In addition to such passive cyber-propaganda, the different party's supporters are also hacking into web pages in order to leave messages detailing their support. Examples are shown in figures 3 and 4 below. The reason for attacks is that, for many individuals, it is the only way in which they can attack what they see as being the enemy. Many of the attacks have caused only minor inconivance.

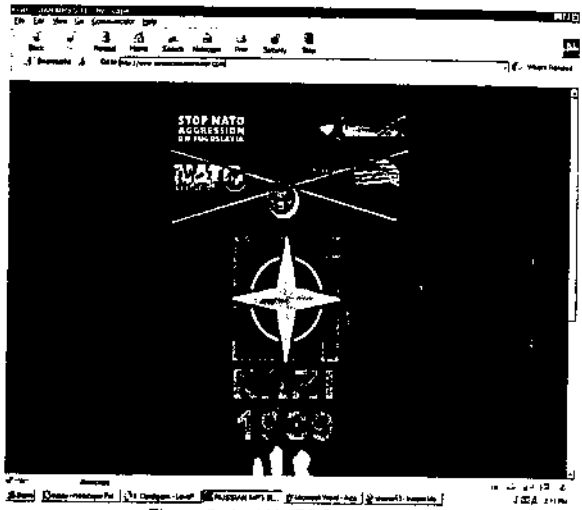


Figure 3: Anti NATO hacking Message

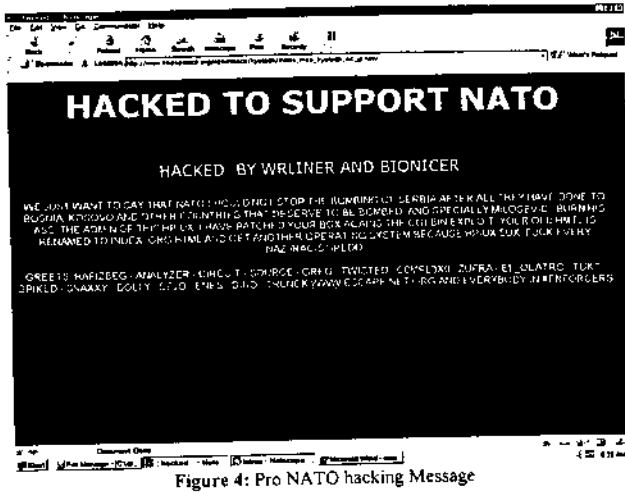


Figure 4: Pro NATO hacking Message

However, some of the attacks have been focused more directly at the parties involved. The official NATO website has been victims to denial of service attacks, at it height 2,000 emails a day were being sent from Yugoslavia, these messages also included macro viruses which for a time affect the NATO e-mail systems (BBC 1999). The aim of the type of attack is to bring down the web-site by sheer numbers of e-mails and disrupt e-mail communication via viruses. The attack was only partly successful.

Whilst these incidents are notable, they are not representative of the more significant damage that cyber terrorism could incur (e.g. the fundamental disruption of society, as referred to at the beginning of this paper). However, the fact that these type of attacks have occurred, and in high numbers, illustrates the actions that can be carried out relatively easily by a small body of highly motivated people using IT as a medium.

5) Responding to the threats

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 (HMSO 1990). 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 (1991) 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 (Warren 1998):

- 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 (NIPC 1998).

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 (Davies 1996).

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 (FBI 1998).

6) Conclusion

The title of this paper referred to the political evolution of the hacker and, indeed, the existence of cyber terrorism lends some weight to the assertion that IT skills can now be employed in active support of a political cause. The discussion has provided some examples of this, in respect of the activities in Kosovo. At the same time, however, we should not automatically class all hackers within the same mindset. A significant proportion of them are not engaging in their activities for political purposes (which is not to say that their actions should not be policed in some way). However, in the

same way that the existence of traditional hackers increases the seriousness with which general computer security is applied, the emergence of the cyber terrorist will mean that stricter controls may need to be considered as standard.

Modern society is significantly dependent upon IT and evidence suggests that this is hardly likely to change in the years ahead. In view of this, it is vital that we are aware of threats such as those highlighted by this paper and take appropriate steps to protect the infrastructure upon which we are reliant.

References

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

Audit Commission. 1990. *Survey of Computer Fraud & Abuse.*

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

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.

BBC, 1999. "Kosovo Info Warfare Spreads", Science/Technology News, BBC web news, 1 April, 1999.

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

Caelli, W., Longley, D. and Shain, M. 1989. *Information Security for Managers*, Stockton Press, New York, USA.

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

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

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

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

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

Malik, I. 1996. *Computer Hacking: detection and protection.* Sigma Press, UK, ISBN 1-85058-38-5.

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

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

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

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

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.

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

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

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

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