IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP4971

Developing New Strategies to Combat Cyber-Terrorism

Christopher Beggs
School of Multimedia Systems, Monash University, Berwick, Australia

Matthew Butler
School of Multimedia Systems, Monash University, Berwick, Australia, matthew.butler@infotech.monash.edu.au

ABSTRACT

Terrorism is no longer a concern for only a religious or ethnic few. It is now a very real threat to the entire global community. A major factor in this widespread concern is the recent emergence of technologically based terrorist activity, or cyber-terrorism. This study provides a brief history of cyber-terrorism, along with discussion of this new threat. Contemporary security measures are discussed, acknowledging fundamental flaws not only in these technologies, but in overall strategies being used. This will form the basis for the major focus of this research: a suggested nine point security plan, aimed at developing new strategies in the fight against cyber-terrorism.

INTRODUCTION

In recent years, governments, organisations and individuals have become faced with a new threat: cyber-terrorism. This has brought about many new areas of concern for governments and organisations across the globe, where they now realise that their critical infrastructures are threatened from new directions. This has been especially highlighted since the devastation of September 11, 2001, with an increase in awareness and alertness of online security, as it was shown that terrorists could exploit new vulnerabilities using recent Internet technologies. The possibility of cyber threats and attacks on our critical infrastructures appeared to be very real concerns.

Although these concerns have caused organisations to become more aware and alert, many are no longer sure if their current technologies, methods and strategies are adequate in preventing future cyber attacks. This has raised the question of whether new solutions and prevention measures are needed in order to fight cyber-terrorism. Organisations are now realising that new technologies, assumed to prevent cyber-attacks, in fact have their own pitfalls and vulnerabilities. As the need to secure technological infrastructures and information assets from cyber attack increases, it must be acknowledged that more than simply investing in new technologies, organisations must develop complete strategies, solutions and methods.

CYBER-TERRORISM DEFINED

There are varying definitions of cyber-terrorism. Lawson (2002) highlights the testimony of Dorothy E. Denning, during her appearance before the Special Oversight Panel on terrorism, where she described it as "the convergence of terrorism and cyber space …unlawful attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objections. Further, to qualify as cyber-terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear".

Likewise, according to the U.S. Federal Bureau of Investigation (FBI), cyber-terrorism is "any premeditated, politically motivated attack against information, computer systems, computer programs, and data, which results in violence against non-combatant targets by sub-national groups or clandestine agents" (Techtarget Network, 2003). The National Infrastructure Protection Centre (NIPC) similarly defines cyber-terrorism as "a criminal act perpetrated through computers resulting in violence, death or destruction and creating terror for the purpose of coercing a government to change its policies" (Berinato, 2002).

Lewis (2002) suggests that The Centre of Strategic and International Studies takes the definition one step further, specifying that cyber-terrorism is "the use of computer network tools to shut down critical infrastructure". An obvious example may be the blocking of emergency communications, or the severance of electricity or water supplies.

It is important to note that cyber-terrorism is not the same as hacking. Cyber terror attacks are typically premeditated, politically motivated, perpetrated by small groups and designed to call attention to a cause, spread fear, or otherwise influence the public and decision-makers. Hackers however break into computer systems for many reasons, although generally to display their own technical prowess or demonstrate the fallibility of computer security. Some online activists say that hacking activities such as defacing Web sites are "disruptive but essentially non-violent" (Council on Foreign Relations 2003).

Cyber-terrorist attacks by definition also differ from computer viruses. Computer virus attacks generally result in a denial of service (DOS), where a user or organisation is deprived of the services of a resource they would normally expect to have. Lawson (2002) suggests that it is important to make distinctions between the two, as the level of response required to combat the attack obviously varies.

Although there are obvious distinctions between cyber-terrorism and its less damaging counterparts, many experts say that they may be linked in launching coordinated attacks and may be the most effective use of cyber-terrorism (Council on Foreign Relations 2003). Hackers and viruses could be used to cause diversions or slow down systems, while the terrorist element could be disabling critical infrastructures and destroying data.

The possibility of this has been made more real by the events of September 11, 2001. It is believed that the al-Qaeda network used internet technologies and communications to coordinate its activities, as well as obtaining critical plans. Security technologies such as encryption and stenography were used to disseminate this information in the public arena. Although, by strict definition, this activity is not cyber-terrorism, it does highlight the real threats that exist in the use of technology to orchestrate terrorist activity.

ISSUES WITH CURRENT TECHNOLOGIES AND STRATEGIES

Organisations are currently questioning the adequacy of their current hardware and software, which they are using to protect themselves from cyber attacks. Current technologies such as firewalls, password protection systems, secret key encryption (3DES), public key encryption (RSA), stenography, intrusion detection systems, Secure Socket Layer (SSL), IPSec, access control lists (ACL) and other security protocols are being implemented by organisations today to protect themselves from outsiders and potential cyber threats.

These technologies, however, are not proving to be the solution to the prevention of low level attacks. New viruses continually ravage

"protected" systems worldwide, with the "Blaster Worm" of August 2003 being a perfect example. Although contained in many systems by higher level security technologies**,** the virus was still able to affect millions of organisations and general computer users. Even though a great number of technologies exist to prevent cyber based attacks, the "Blaster Worm" was able to cause great chaos and disruption.

Similarly, the many reports of hacking are also testament to this fallibility. Even the FBI has shown that despite sophisticated technologies, vulnerabilities exists. The reality is that if these technologies alone are not able to contain the plethora of hackers and viruses, then cyber-terrorists would be able to bypass firewalls, password protections systems and the like. The United States government recently tested, and proved, the vulnerability of their infrastructure by creating a team with the sole purpose of infiltrating their systems. Called 'Eligible Receiver', this was an internally organised project, designed to find weaknesses within their critical systems. Although many details about Eligible Receiver are still classified, it is known that the team was able to infiltrate and take control of the Pacific Command Centre computers, as well as power grids and 911 systems in nine major U.S cities (PBS 2003).

Likewise**,** current technologies also provide little resistance to other, less obvious, immoral activity. Investigators discovered an al-Qaeda computer containing software and connections to a site containing specific information about digital switches within power and water company system infrastructures. It showed how al-Qaeda was doing research through open, available resources to learn more about US critical infrastructure and how to exploit it. Along with the growing sophistication of hacking tools available on the Internet, many experts are concerned about terrorists such as al-Qaeda adopting high level cyber tactics (PBS 2003).

It is important to acknowledge that the technology available today is helping organisations secure their information from viruses, hackers, and cyber related threats and attacks. Although this protection is limited to a certain extent, governments and organisations are certainly using these technologies to assist in the protection of critical infrastructures and organisational assets. For the majority, this security protection is quite sufficient and effective. However, critical infrastructures such as gas, electrical, banking, defence and water systems, are likely targets for terrorists and require more effective solutions to secure their information systems. O'Brien (2002 p.13) cites Condoleezza Rice who states, "it's a paradox of our times that the very technology that makes our economy so dynamic and our military forces so dominating also makes us more vulnerable".

In February 2002, more than 50 distinguished scientists and national leaders wrote an open letter to U.S. President Bush, calling for a "Cyber-Warfare Defence Project modelled in style of the Manhattan Project". The signatories to this letter warned that the clock was ticking and that the U.S was at grave risk of a cyber attack "that could devastate the national psyche and economy more broadly than did the September 11 attack" (PBS 2003). This open letter increased the US level of alertness and shortly afterwards, President Bush released a national strategy to secure cyberspace. The strategy identified threats and vulnerabilities at five levels**:** home users and small business; large enterprises; critical sectors/infrastructures; national issues and vulnerabilities; and at a global level. The strategy involved methods and measures that could be implemented and be used to secure and protect governments, large enterprises and home users.

A 'National Strategy to Secure Cyberspace' has also been introduced, looking at all sectors, both public and private. Again, technology was not the sole focus of this document. Clarke (2002) discusses this document, highlighting that focus within the Strategy instead has been placed on an architecture coordinated by the Department of Homeland Security (DHS) for analysing and warning incidents of national significance, promoting continuity in government systems and private sector infrastructures and increasing information sharing across and between organisations to improve cyberspace security. Similarly the strategy promotes security awareness and user training, as well as working in coordination with appropriate federal, state and local entities, and private organisations providing awareness campaigns and stay safe online campaigns as well as award programs for those in industry making significant contributions to security.

As highlighted earlier, certain technologies and strategies are indeed in place to help prevent the war on cyber-terrorism. Organisations need to evaluate and assess these current technologies and methods to see if they are adequate in preventing cyber attacks, as well as assessing new technologies to counter attack and prevent cyber-terrorism. These technologies and methods may not be adequate for many organisations; new prevention measures, counter attack methods and solutions may need to be acquired. What the National Strategy, as well as the open letter to President Bush, acknowledge is that in the last eighteen months, emphasis is being placed on the need for strategy, rather than relying on just technology, to protect systems from cyber attacks. Focus must be placed on solving the problems, rather than the reactive approach of developing technologies to simply slow down or stop infiltration.

SOLUTIONS AND PREVENTION MEASURES

Several authors have acknowledged the fundamental concerns raised earlier, and as a result have offered ideas for tackling the problem of cyber-terrorism, rather than simply relying on further technological development. O'Brien (2002 p.26) recognises the inadequacies and has defined a set of initiatives using the standard information security paradigm of *Deterrence, Prevention, Detection and Reaction*. On the same note, Vatis (2001) claims that system administrators and governments should be on high alert for the warnings of impending hostile cyber activity, particularly during periods immediately following military strikes or covert operations. He believes systematic and routine risk assessments of information infrastructures provide a good starting point for effective risk management and thus should be a priority. Best practices for maintaining systems should be followed as a tenet of any organisations standard procedures; operating systems and software should be regularly updated; strong password polices should be enforced; systems should be 'locked down'; all unnecessary services should be disabled; antivirus software should be installed and kept up to date; high fidelity intrusion detection systems and firewalls should be employed.

Although O'Brien and Vatis provide some solutions and preventative measures to stop terrorism, these strategies and solutions are not complete in their scope. Other solutions may be needed in order to prevent cyber attacks. A complete strategy must encompass policy, procedure, technology, as well as various other important aspects. Hershman (2000) suggests that countries that refuse to turn in cyber-terrorists can be disconnected from the Internet 'pipelines' which connect the globe, resulting in detrimental effects on organisations within these nations. It is important to acknowledge however that developing truly global treaties has countless barriers - many of which are seen everyday in other global affairs and United Nations endeavours. Clarke (2002) points out that the fact that the vast majority of cyberspace is neither owned nor operated by any single group, either public or private, presents a challenge for governments and online organisations. However**,** in simply attempting to develop such a strategy, this can provide benefits in opening communication channels and creating dialogue between nations on the global implications of the issue.

The development of treaty and policy can also encourage greater participation from the private sector. More organisations within the private sector need to co-operate with government bodies and anti-cyber-terrorism organisations to help prevent cyber related threats and attacks occurring. Greater involvement from private sector organisations would aid in aligning security strategies and policies, as well as providing more financial support to help fund terrorism treaties and other anti-cyber-terrorism organisations. It is important that the private sector acknowledge their responsibilities in tackling the issue of cyber-terrorism. Given their critical role in developing leading edge technologies relating to security, it is only logical that the private sector invest in this crucial area. Their duty of care to clients and corporate responsibility must extend beyond basic day to day obligations.

Also within both public and private sectors managers and individual employees need to take responsibility for their own security measures. Employees need to understand the importance of secure passwords, virus prevention software, and the like. Governments and organisations need to have user policies created and enforced, covering appropriate use, security issues, as well as promoting vigilance in technological activity.

These policies need to be concise and understandable to all employees that work in the organisation. These policies must also ensure the education of staff. Educating managers and individual staff will constitute effective security enforcement and will contribute towards the safety and security of their information assets. If employees are educated about the necessary measures and security mechanisms needed to prevent cyber-terrorism, they will be prepared and be able to react if such cyber attacks occurred.

The ideas raised here can be summarised into a nine-point security plan, *"SPECTR FCC"*; embracing the key elements of Strategy; Policy; Education; Communication; Technology; Responsibility; Funding; Commitment; and Co-operation. The plan is derived both from literature review and case study, and also acknowledgement of fundamental flaws within contemporary security measures. The plan makes possible recommendations that governments, organisations and individuals could use to combat cyber-terrorism.

Strategy must be developed by Governments and other organisations. This must focus on implementing and developing an appropriate 3-5 year plan to protect critical infrastructures against cyber-terrorism. A strategy must incorporate all of the following elements, not only the development and implementation of new technologies, as this has proven to be an ineffective and flawed approach.

Policy ensures that appropriate behaviours are documented and understood by all managers and employees, as well as documenting the necessary security mechanisms that are set in place. In addition to this, effective managerial communication and operational planning are needed by all employees within the organisation.

Education of all managers, employees and individuals needs to be undertaken on the security mechanisms and strategies being used within the organisations. If more employees are educated in the security mechanisms they are using, this will lead to a better understanding of the security mechanisms in place, as well as going a long way in protecting their information assets.

Communication between organisations is essential to prevent and deter cyber attacks against critical infrastructures, as well as promote the creation of policy. Communication between all sectors can close back doors, access holes and other areas of exploitation. If organisations are warned of potential vulnerabilities within software, then they can take the necessary preventative measures.

Technology improvements are still required but do not need to be the centre point of a cyber-terrorism strategy. Less focus should be placed on technology, as technology continues to show signs of vulnerabilities within organisations. However it still has a major role in protecting organisations from cyber attacks. The necessary security technologies such as firewalls, encryption, and intrusion detection systems need to be implemented by organisations to protect themselves against deadly attacks.

Responsibility needs to be taken not only by managers, but by all employees and individuals. If organisations are not taking responsibility in protecting their information assets then cyber-terrorism will continue to be a threat towards organisations.

Funding is needed towards organisations like DHS, AusCert, terrorism treaties and other anti-cyber-terrorism organisations. This funding also needs to come from the private sector, as they too have a duty of care to individuals world wide, but also as they must be a primary contributor to cyber-terrorism policies and technologies.

Commitment from all sectors is essential in order to fight cyber-terrorism. Without commitment from everyone, organisations will continually be faced with cyber threats and cyber attacks. If the private sector is not willing to participate and be committed in stopping cyber-terrorism, the creation of policy and facilitation of global communication becomes impossible.

Co-operation is vital between all organisations if they want to protect their information assets. Without co-operation**,** organisations will be faced with communication barriers and will not be able to collaborate, share ideas and make improvements towards online security.

The plan may have its own limitations, but further research would examine the validity of the proposal, embracing thorough analysis and discussion between governments and organisations. It must also be acknowledged that some of the ideas and preventative measures raised have obvious ethical, legal and privacy issues associated with them. Issues of privacy have always been at the forefront of combating terrorism, and since the events of September 11, they have again been placed in the spotlight. Whilst these issues require much deeper examination than is possible here, it is important to highlight that the authors acknowledge these issues, and intend to consider them in the development of comprehensive cyber-terrorism strategies.

CONCLUSION

Although some security technologies, methods and strategies have been developed and implemented in the hope of curbing cyber-terrorism, organisations are becoming more vulnerable as new technologies are developed. Even though these technologies are playing a large role in trying to mount a war on cyber-terrorism, they are also providing cyber-terrorists the opportunity to exploit critical infrastructures across the globe. As a result, future plans in dealing with this critical issue need to consider not only technology but importantly they also need to encompass the development of strategy, policy, open communication channels, as well as developing and assigning responsibility – with the aim of increasing cooperation between the public and private sectors of all countries.

The proposed nine-point plan ("*SPECTR FCC*") is intended to acknowledge issues in current strategies (or lack thereof) being employed in the fight against cyber-terrorism. Although not definitive, it is designed to address fundamental concerns with current approaches and provide the framework of a complete strategy for combating the problem of cyber-terrorism. Ultimately, co-operation from everyone will raise the awareness of all issues and help counter such threats, thereby building a safer and more secure environment for all.

REFERENCES

Australian Computer Emergency Response Team Copyright 2002-2003, *AusCert* (Online) Available: http://www.auscert.org.au (Accessed 2003 August 20)

Author Unknown (2001)" Fighting Cyber Terrorism - Where Do I Sign Up?" *SANS Institute* (Online) Available: http://www.sans.org (Assessed 2003, July 12).

Berinato, S. (2002), "The Truth About Cyberterrorism," *Cio Magazine*. (Online) Available: http://www.cio.com/archive/031502/truth_content.html (Accessed 2003 April 10).

Clarke, R. A.. (2002) "The National Strategy to Secure Cyberspace" *White House* (Online) Available: http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf (Accessed 2003 July30).

Council on Foreign Relations Copyright 2003 *Terrorism Answers* (Online) Available: http://www.terrorismanswers.com (Accessed 2003 16 April).

Hershman, T. (2000), "Cyber-terrorism Conference for International Cooperation" *Internet News* (Online) http://www.internetnews.com/bus-news/article.php/9691_533311 (Assessed 2003, August 14).

Lawson, M. S. (2002) "Information Warfare: An Analysis of the Threat of Cyber-terrorism Towards the US Critical Infrastructure" *SANS Institute* (Online) http://www.sans.org (Assessed 2003, April 12).

Lewis, J. A. (2002) "Assessing the Risks of Cyber-terrorism, Cyber War and Other Cyber Threats" *Centre for Strategic and International Studies* (Online) http://www.csis.org (Assessed 2003,May 15)

O'Brien, K. 2002, "Workshop on The New Dimensions of Terrorism," *Institute of Defence and Strategic Studies*, Nanyang Technological University, Singapore

Public Broadcasting Service (PBS) (2003) "Cyber War" *Frontline: Cyber War!* (Online) Available: http://www.pbs.org/wgph/pages/frontline/shows/cyberwar (Accessed 2003, 16 July).

Techtarget Network (2003) *whatis.com* (Online) Available: http://www.whatis.com (Accessed 2003 15 April).

Vatis, M. (2001), "Cyber Attacks During The War on Terrorism: A Predictive Analysis" *Global Community Center* (Online), (2001) http://www.globaldisaster.org/cyberattacks.pdf (Assessed 2003, April 10).