Cyberterrorism: The Next Arena of Confrontation

Dr. George K. Kostopoulos, Consultant - Educational and Technology Projects, Athens, Greece
george@kostopoulos.us

Abstract

This paper presents a research conducted over the increasing dangers of cyberterrorism. It discusses the cyberterrorism parameters - the cyberterrorists, the attacks, and the countermeasures – as well as the Internet's physical security. The paper sounds an alarm over the current accessibility of critical intranets via the Internet, and points out that the risks in this practice outweigh any possible benefits. Concern is also raised over the security of Internet's physical infrastructure, suggesting increased redundancy and that countries have more physical entry points into cyberspace. The paper concludes with two recommendations. One is the physical isolation of the Internet from critical intranets, and the other is the development of an Internet SCADA to oversee the Internet's performance in the U.S. cyberspace.

> *"In the case of cyber war, you really can't tell whether the enemy has good weapons until the enemy uses them."*
> (Clarke[1] in Kirk, 2003)

Keywords: cyberterrorism, information assurance, internet security, malware, scada, botnet, nimda.

1. Introduction

The cyber space – the world's Internet, intranets and extranets – has become a most valuable and at the same time most critical resource. Its rapid development has left its defenders behind, and today the world stands vulnerable to attacks that can cause unprecedented damages. Experts have described the potential impact of cyberterrorism in very scary terms[2]. In the words of a power distribution expert *"… loss of power for six months or more …over a very big area … is a possibility"* [1]. In the words of a hacking expert: "*If you do the job correctly, there are no fingerprints and nobody can trail you back.*" [2].

Cyberterrorism is the next arena of confrontation. While rogue groups are advancing their cyber warfare skills, legitimate governments are developing their own cyber defense capabilities to be able to face off cyber attacks. This rigorous exercise of developing cyber defenses inherently creates cyber offensive capabilities.

2. Cyberterrorism Parameters

Cyberterrorism parameters may be grouped into three categories; the cyberterrorists, the attacks, and the countermeasures. With time, all three, each in its own way, will become more and more sophisticated and powerful, with the countermeasures trailing the attacks.[3]

A distinction has to be made among the three basic types of cyberterrorists. The *professionals*, those who, by order of their sponsors, aim at inflicting physical or cyber damage onto victim's resources, the *amateurs*, who find pleasure in applying cyber graffiti defacing corporate or government websites, and the *thieves,* who have immediate personal illicit economic benefit from their actions.

The *professionals* are cyberterrorists who operate behind a variety of facades – political extremists, religious fanatics, revolutionaries, and the like [3].

The fact remains that the cyberspace allows the cyberterrorists anonymity, and the potential impact of their attacks, as well as their timing, is unpredictable. It must be recognized that the technical education, the experience and the expertise of the cyberterrorists, especially of the *professionals*, parallels that of the networks design experts. In addition to this technical background, cyberterrorists also develop knowledge on the network architecture of the victim's resources. It must also be recognized that *professionals* are not malevolent volunteers, but well sponsored operatives of political, military, or economic interests; state or private. *"The threat of terrorism will grow in the*

[1] Richard Clarke was Director of Cyber Security in the White House, USA, and a strong alarmist on cyberterrorism.
[2] Quotations appearing in this page have come from a very interesting interview broadcast by the PBS, Public Broadcast System.

[3] Throughout this research, practically all sources were considering cyber defense as *terra incognita*.

New Millennium … (and) … *cyber attacks … are truly international…"* [4][4].

While it is wise to protect network and databases, and other resources, against far away cyberterrorists, *"…for most organizations insider threats constitute the dominant threat to networks and end-systems[5]"* [5]. Therefore a comprehensive cyber protection plan is needed.

3. Attacks

Cyber attacks can be broadly classified into Internet based and into physical. The latter are very underestimated. Through Internet based attacks intruders may spread malware, snoop or destroy data, or cause denial of service[6]. Thus, disrupting or damaging the Internet infrastructure, or the infrastructure of organization that are Internet accessible. Physical attacks aim at the physical side of the Internet, nodes and communications media, through physical offensive means.

Internet Based Attacks

Malware made their first major presence in the Internet in 2000, but it was in 2003, when the world realized what a cyber attack can really do. A worm

named *Slammer* (alias *Sapphire*) attacked the Internet (US, Korea, Japan, Finland, and many more countries). According to the coverage in the media, the *Slammer* entered the Microsoft IQL Server, through a *hole*[7]. The spread took place in 30 minutes and affected a wide variety of networks including banking and airlines. "*The Slammer worm penetrated a private computer network at Ohio's Davis-Besse nuclear power plant in January and disabled a safety monitoring system for nearly five hours, despite a belief by plant personnel that the network was protected by a firewall. (The Slammer) will stay in history, as the fastest spreading worm."* [6].

The question is: was the *hole* a technical oversight the cyberterrorist discovered and capitalized on?
Or was it a *trapdoor*[8] and information about its presence leaked out? A new release of the Microsoft SQL Server 2000 "…i*s now available for free. This release includes the fixes for the Slammer (W32.slammer) worm"* [7]. Fig. 1 illustrates on a world map *Slammer's* coverage [8]. Subsequently, and until the present, malware made appearances followed by appropriate patches provided by the industry's antivirus *guardians*. In 2001, however, 300,000 computers were affected by the *worm* named *Code Red.* Even the White House website was infected. *Red Code* entered the Microsoft Internet Information Server, IIS, through a *hole*. It is not known if it were an inadvertent hole, or a deliberate *trapdoor*. Eventually, a patch was developed and Microsoft made it available to the public [9].

Again in 2001, millions of computers were affected by the *Nimda.* It was also a worm entering networks via emails multiplying itself in computer servers. *"The only safe way to recover from the system compromise is to* (re)*format the system drive(s) and reinstall the system software from trusted media (such as vendor-supplied CD-ROM)… after the software is reinstalled, all vendor-supplied security patches must be applied* (immediately and offline)*"* [10].

Via the Internet, numerous other malware found their way into millions of computer creating inconvenience and costing billions in productivity loss.

Preceding attacks, cyberterrorists intrude potential victims' network facilities to identify possible

[4] This article by Paul Rogers of the FBI was published in the U.S. Foreign Policy Agenda. An Electronic Journal of the U.S. Department of State, Vol. 6, No. 3, November 2001.

[5] The International Telecommunications Union, ITU, has conducted a study *Creating Trust in Critical Network Infrastructure: Canadian Case Study*. The study explored the Canadian telecommunications environment, particularly data communications, and assessed critical infrastructures including the Internet, and their interdependencies.

[6] DoS, Denial of service is a scheme where the attacker *enslaves* through malware thousands of computers around the world and directs them, like mean dogs, against the victim's server. The server's capacity is saturated and bona fide visitors are left outside.

[7] *Hole* is a term used in the software development lingo to imply a path that bypasses the normal security checks and takes control of the attacked system.

[8] *Trapdoor* is another term meaning an intentional *hole*. Programmers often include *trapdoors* in their designs mainly for troubleshooting purposes. Normally *trapdoors* are deleted prior to software release.

vulnerabilities. In one case in California, a municipality's website had repeated intrusion attempts from overseas locations, apparently testing the rigor of the networks defense. It appeared that the intruder was collecting information on utilities and emergency systems. The respective SCADA,[9] system recognized the intrusion attempts and appropriate measures were taken. Subsequent investigation concluded that the intrusions originated in the Middle East and South Asia [11]. Of course, the origin of the intrusions does not in any way reveal the true identity of the intruders neither that of their sponsors.

Besides spreading malware, and snooping or damaging databases, cyberterrorist also create *botnets*[10] of thousand of computers and direct them to attack predetermined sites at predetermined times. Naturally, the servers at those sites get saturated and cannot respond to bona fide traffic.

Physical Attacks

It is surprising that out of the thousands of pages of literature reviewed for the preparation of this paper; practically nothing was found on the vulnerability of the physical Internet infrastructure.

After all, doesn't the Internet have a physical infrastructure? Maps of the Internet backbone, appearing in Fig. 2, clearly show the paths of the transmission media and the location of the major Internet nodes. Don't these resources deserve extra protection? Yet, nowhere is it being emphasized, or even mentioned, that this is another of Internet's vulnerabilities.

The Taiwan earthquake that *"…seriously affected"* Internet connections, and *"…disrupted 98% of Taiwan's communications with Malaysia, Singapore, Thailand and Hong Kong...."* demonstrated that it does not take a coordinated cyberterrorist attack to shut down the Internet [12].

Physical damage intentional, or unintentional, can have the same effect. A cyberterrorist does not consider damage to the Internet's physical infrastructure an *off limits* activity.

4. Countermeasures

Countermeasures for the above discussed threats and attacks possibly exist, or can be found. Some of these countermeasures are anti-malware[11], backing up of files, use of intelligent SCADA, or use of encryption.

It is suggested that *"…a minimum standard of security for computer networks."* be defined and be applied across Internets thousands of subordinate networks [13]. But what good will the countermeasures do if the Internet is shut down? Or our Internet server is saturated by ill-intended requests?

As for countermeasures to physical attacks onto the Internet infrastructure, the best defense is multiplicity of Internet resources – more nodes, additional transmission media paths (preferably wireless media), and more DNS[12].
In the literature one may find numerous scenarios of "*Potential CyberTerrorist Acts*". A report by the Institute for Security and Intelligence, in a long list of potential cyber attacks, claims that "*Cyberterrorists* (via the Internet may). . . *remotely access the processing control system of a cereal manufacturer, and change the levels of iron supplement , and … kill the children …* (also) *remotely alter the formulas of medication at pharmaceutical manufacturers... the cyberterrorist does not have to be at the factory to execute these acts"* [14].

If so many horrible disasters may happen because a company's intranet is accessible by the Internet, then why should that intranet be accessible? A study by the Business Roundtable sounds an alarm. As the Internet stands today, there is no *early warning* system for pending disasters, neither is there allocation of coordinate responsibilities *"…in reconstructing the Internet infrastructure*" [15].

The best countermeasure to cyberterrorism is the physical isolation of the Internet from the intranets of sensitive industries, government agencies, and other entities that must remain out of *harm's way*.

5. Conclusion

[9] SCADA, Supervisory Control And Data Acquisition systems, oversee the performance of supervised systems looking for unusual activities or patterns that may lead to possible intrusion attempts.

[10] Botnet is the abbreviation of robot networks. These are networks a cyberterrorist infects with a malware and remotely controls them.

[11] It appears that there is a race between software and malware, with the malware having a constant three month lead.

[12] DNS, domain name servers, are located throughout the Internet converting domain names, such as www.umuc.edu to its respective Internet numerical address, which in this case is 131.171.8.112. UMUC can be equally reached at http:// 131.171.8.112

The Internet is not only virtual, but it is also physical. It is being implemented by an extensive and expensive physical telecommunications infrastructure with certain most critical components, such as the DNS. Damage to the DNS immediately paralyzes the domain name system, and subsequent access to websites.

It needs to be pointed out that cyber threats do not all come as ones and zeros. The threats also come as damage to the physical facilities that support the Internet – communications media, mainly the *backbones*, the thousands of interconnecting nodes and the hundreds of domain name servers.

The Internet is an integral part of today's society. It is a useful social tool, as well as a most effective *front office* for commercial transaction processing. Therefore its availability on a 24/7 basis is beyond any compromise, and its security is a global responsibility.

Cyberterrorists are not *lone strangers*; they are teams of professionals in the service of resourceful sponsors. Most probably, some of them are former colleagues of ours who *crossed the line*. They cannot be outsmarted, but they can be kept at a physical distance.

6. Recommendations

The intranet-Internet interweaving is a very volatile mix. *"The vulnerabilities of the PTN[13] and Internet are exacerbated by the dependence of each network on the other. …Thus, vulnerabilities in the PTN can affect the Internet, and vulnerabilities in Internet technology can affect the telephone network"* [16].

The study of the Business Roundtable, mentioned above, also states that *"…the United States is not sufficiently prepared for a major attack … that would …* (incapacitate)*… large parts of the Internet*". The report sounds another alarm stating that *"… government … and …industry…are not in a position …to restore Internet services"* [17]. As a result of this research the following two recommendations are being made:

Recommendation One: Physical isolation of critical intranets and Internet.

Any nation's critical infrastructures – communications, power grids, water supplies, gas lines, military, and the like - and their networks must have nothing to do with the Internet. Such infrastructures must have their own intranets, accessible only from selected locations and physically and virtually secure.

It is convenient and inexpensive to tap onto Internet's omnipresence and access resources; but the created vulnerability is a price no country can afford. The recommended deployment of exclusive-access networks carries a cost. However, this cost is merely a fraction of the damage a knowledgeable cyberterrorist can cause to critical resources, should they be Internet accessible.

Recommendation Two: The development of an Internet SCADA.

As for the Internet itself, this research recommends that a comprehensive SCADA be progressively configured and deployed *over the Internet*, in order to oversee the traffic, possibly recognize disasters in the making, and hopefully avert them. Considering that *"Stealth and pre-operational surveillance are important characteristics known to precede a computer attack…*" a supervisory system may provide most needed early warnings of risk.[18].

7. References

(The availability of all referenced URL was confirmed on November 2, 2008)

[1] Weiss J. (Speaking in) Cyber war [Television series episode] Kirk, M. & Gilmore, J. (Producer), Frontline. PBS. Park Foundation. (2003). http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/etc/script.html

[2] Hacker A. (Speaking in) Cyber war [Television series episode] Kirk, M. & Gilmore, J. (Producer), Frontline. PBS. Park Foundation. (2003). http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/etc/script.html

[3] Duell, S. (2001). Cyberterrorism. American Society for Industrial Security: San Francisco Bay Area Chapter.
http://www.sfasis.org/archives/2001/v7i10a2.htm

[4] Rodgers, P. (2001, November). Protecting America against cyberterrorism. U.S. Foreign Policy Agenda. Vol 6, Issue 3. United States Department of State. p17.
http://usinfo.state.gov/journals/itps/1101/ijpe/ijpe1101.pdf

[13] PTN, Public Telephone Network

[5] Harrop, M. (2002) Canadian case study. Document CN 107. Workshop on creating trust in critical network infrastructures. p 38. International Telecommunication. Union. Seoul, Republic of Korea. http://www.itu.int/osg/spu/ni/security/docs/cni.07.do

[6] Poulsen, K. (2003, August). Slammer worm crashed Ohio nuke plant network. Security Focus. http://www.securityfocus.com/news/6767

[7] Microsoft. (2007). Microsoft SQL server 2000 desktop engine. (MSDE 2000) Release A. Download Details. Microsoft Download Center. Microsoft Corporation. http://www.microsoft.com/downloads/details.aspx?familyid=413744D1-A0BC-479F-BAFA-E4B278EB9147&displaylang=en

[8] PBS. (2003). Cyber war: The geographical spread of the slammer worm. Frontline. PBS. Park Foundation Image. http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/slammermap.html

[9] CERT Coordination Center. (2001). (CRA) Code red alert. Carnegie Mellon Software Engineering Institute. http://www.cert.org/congressional_testimony/CRannounce.html

[10] CERT Coordination Center. (2001). CERT advisory - CA 2001-26 Nimda worm. Carnegie Mellon Software Engineering Institute. http://www.cert.org/advisories/CA-2001-26.html

[11] Hsiung C. (Speaking in) Cyber war [Television series episode] Kirk, M. & Gilmore, J. (Producer), Frontline. PBS. Park Foundation. (2003). http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/etc/script.html

[12] BBC (2006). Asia communications hit by quake. BBC News: Asia-Pacific. British Broadcast Corporation. http://news.bbc.co.uk/2/hi/asia-pacific/6211451.stm

[13] Ford, R., Gordon, S. (2002). Cyberterrorism? Symantec Security Response. Symantec Corporation. p. 10. http:www.symantec.com.avcenter/reference/cyberterrorism.pdf

[14] Collin B. The Future of Cyber Terrorism: Where the Physical and Virtual Worlds Converge, Institute for Security and Intelligence. (2004). http://www.crime-research.org/library/terrorism02_2004.html

[15] Business Roundtable. (2006). Essential steps to strengthen America's cyber terrorism preparedness. p.2. http://www.businessroundtable.org/pdf20060622002CyberReconFinal6106.pdf

[16] Schneider B. et al., Critical Infrastructures You Can Trust: Where Telecommunications Fits, 26th Annual Telecommunications Policy Research Conference. Critical Infrastructures You Can Trust p. 7. http://radiata.cs.columbia.edu/~smb/papers/tprc.pdf

[17] Business Roundtable. (2006). Essential steps to strengthen America's cyber terrorism preparedness. p.1. http://www.businessroundtable.org/pdf20060622002CyberReconFinal6106.pdf

[18] Wilson, C. (2003). Computer attack & cyber terrorism: Vulnerabilities & policy issues for Congress. Congressional Research Service. Order Code RL 32114. http://www.fas.org/irp/crs/RL32114.pdf