Muslim Internet Service Providers – Cyberterrorist Highways

Captain Douglas W. Craddock
Naval Postgraduate School

MUSLIM INTERNET SERVICE PROVIDERS – CYBERTERRORIST HIGHWAYS

The Internet continues to grow exponentially. It is estimated that over 1 billion people – one-sixth of humanity – will be on-line by 2005, two thirds of them abroad. Along with this increase in net users, has come an exponential increase in hacker attacks. Merkle (1998) relates that a hacker will most likely be a member of a cybergang that is “organized into “rings” or “cells” (p. 87). He further states:

Why do people join? In cyberspace, the reasons can range from interest in disseminating underground computer information as a sort of “trading post” to exchanging illegally duplicated software or “warez.” Others may feel it necessary to travel in packs or “crews” for personal protection and/or to assault institutions or individuals far more effectively. They settle scores this way, both virtual and actual. (p. 88)

Hackers range the spectrum from complete amateurs at the bottom, to semi-serious part-time hackers in the middle, to the Internet terrorist at the top. “The absolute worst-case scenario is the professional terrorist/hacker” (Merkle, p.74). In addition to knowing computer operating systems inside and out, “he may actually be paid or retained by an individual or group, as in the case of corporate espionage, or he may find cyberterrorism to be his true calling in life and do it to achieve his own ends, whatever they may be” (p. 74). When you couple this individual’s technical expertise with computers to a belief in a cause, such as radical Islam, you may have a cyberterrorist with the skills, knowledge, capability, and intent, to cause catastrophic disruption when and wherever he chooses.

Woven into this cybergang culture are terrorist organizations that realize the capability of using cyberterror to strike anonymously at their enemies. Whine (1999) notes that:

In cyberspace, national borders are no longer relevant. Electrons do not stop to show passports. Potentially serious cyber attacks can be conceived and planned without detectable logistic preparation. They can be invisibly reconnoitered, clandestinely rehearsed, and then mounted in a matter of minutes or even seconds without revealing the identity and location of the attacker. (p. 4)

The use of the Internet by hackers/cyberterrorists has been paralleled by the employment of new information and communication technologies (ICTs). These ICTs offer both external and internal connectivity to a worldwide network of like-minded people. As Whine aptly notes, ICTs “allow the diffusion of command and control; they allow boundless new opportunities for communication, and they allow the players to target the information stores, processes and communications of their opponents (p.1). Arquilla and Ronfeldt (1996) have termed the use of ICTs to influence, modify, subvert, disrupt or damage the institutions, population or media
of nation-states as ‘netwar’. Cyberterrorists, if they attain the capability to implement netwar on a broad telephony spectrum, can threaten disruption on a catastrophic scale. In this paper, I will explore why radical Islamist terrorist organizations, including Usamah Bin Mohammad Bin Laden’s (UBL) widespread terrorist organization Al-Qaida (The Base), would use Muslim Internet Service providers, to carry out netwar against targeted nation-states.

**MUSLIM INTERNET SERVICE PROVIDERS (ISPs)**

Muslim owned and/or operated ISPs are present in almost every country in the world today. They provide Internet services ranging from low-speed (56Kbps modem) connections to the Internet, to high-speed (xDSL) connections for individuals and businesses. While most Muslim ISPs are Tier 3 providers – typically servicing only one city, many are established Tier 2 telephony providers - covering a region or group of major metropolitan areas. To gain access to national and international markets, Tier 2 and Tier 3 ISPs buy wholesale access through national and international Tier 1 providers such as Sprint, MCI, British Telecom, among others. This is accomplished through bilateral peering agreements, which allow the exchange of routing information and traffic between networks and the transport of packets to third parties for monetary compensation from the smaller ISP. This static, or default, routing allows the smaller ISP to configure its routers to retransmit all traffic not directly connected to its network via the transit provider’s router. This arrangement allows Muslim ISPs to reach national and international audiences for their customers.

Although Al-Qaida and other terrorist organizations do not have to utilize Muslim ISPs, and in many countries do use other providers, Muslim ISPs in countries such as Pakistan provide conduits to computer savvy personnel who share the same ideology of Al-Qaida, and are potential recruits into the cyberterrorist world. Muslim ISPs also provide the ideological base for various Islamic groups and organizations to present their cause to the outside world through Web sites (the majority use English) and email communications. This gives terrorist organizations ready-made access to a worldwide audience, both in the Islamic Diaspora and beyond it. These Islamic groups and organizations provide the backdrop against which terrorist organizations carry out subversive activities worldwide. In fact, Al-Qaida is able to perform almost every ideological and administrative function of a terrorist organization by using established Muslim ISPs. Trying to stop terrorist organizations’ use of the Internet for subversive purposes is not feasible. As Denning (1999) notes, “forcing them off the Web is impossible, because they can set up their sites in countries with free speech laws” (p. 68).

**COMMUNICATIONS**

Covert communications are the backbone of any terrorist organization. Using Muslim ISPs to reach “cyberspace allows covert communication and anonymity, and anonymity is probably the most noticeable trend in terrorist acts of recent years” (Whine, p. 4). Many Muslim Web pages feature direct links to proxy servers such as Anonymizer.com, Zeroknowledge.com, and Proximate.com. All provide anonymous net surfing and email. Some offer Web publishing and secure dial-up services that include strong SSL encryption between the user and the network. In the case of Anonymizer.com, all user activity appears to come from the Anonymizer subnetwork in San Francisco, California. Data encryption
such as Pretty Good Privacy (PGP) - available at web.mit.edu/network/pgp - is also freely available on the net and easily downloaded and used. Whine states:

Terrorist groups are known to share information and to collaborate with one another through cyberspace. Since such collaboration is inherently risky, and inter-group communication is a target for national security services, the use of encryption has increasingly been adopted. The encryption might be used both to ‘anonymise’ and to authenticate communications. The digital basis of cyberspace communication makes it an ideal vehicle for encrypted communication. (p. 5)

Regan (1999) relates that:

Egyptian members of Mr. Bin Laden’s network are said to have helped devise a communications network that relies on the Web, e-mail, and electronic bulletin boards so that members can exchange information without running a major risk of being caught by US counterterrorism organizations”. (p. 2)

Terrorist organizations, using proxy services coupled with encryption algorithms are able to gather intelligence, plan operations, and direct activities through email and web sites supported by Muslim ISPs. A new tool, which makes it easy to publish information on the Internet anonymously, is the use of Freenet. Cohen (2000) reports that:

Unlike files on the Web, files on Freenet do not have a unique Internet address that specifies the computer on which they are held. Instead, files are distributed around the net on computers belonging to Freenet members. Several copies of each file exist in different places to make it hard to delete them. When a file is stored, it is given a “key”, Freenet’s equivalent of a web address. The software then forwards the data to other servers, but the creator of the file doesn’t know to which. To retrieve a file, users enter the key. Their computer then queries Freenet servers until one is found that has the associated files. If a Freenet user has a copy of a file on their machine, it doesn’t mean they published it. In fact, they might not even know it’s there. Clarke argues that at no point can any one computer user be held responsible for Freenet files, because there is no way of knowing their origin. “It’s a perfect machine anarchy,” says Clarke. “No single computer is in control.” (P. 1)

When tools such as the above become available and more well known, terrorist organizations will have free rein to publish information anonymously, making the Internet even harder to police.

**PROPAGANDA and RECRUITING**

Islamic Web sites, reached through Muslim and other ISPs, provide the perfect front for terrorist organizations to recruit, raise money, and propagandize. Since most countries have established policies of not negotiating with terrorists, and traditional media outlets quickly pull the plug on subversive propaganda, the use of Muslim ISPs allows terrorist organizations to reach their target audience through established Islamic Web sites. Some of these Web sites include Hizb-ut-Tahrir (Islamic Liberation Party), whose UK leader, Omar Bakri Mohammed, provides hardcopy publications, contacts, as well as communiqués of UBL; the Saudi opposition
group, Campaign for the Defence of
Legitimate Rights (CDLR), which posts
information from groups not directly
associated with it; the pro-Iranian
Muslimedia International, which, like many
other sites, posts interviews with UBL; the
Australian based Nida’ul Islam site which
promotes both Jihad and suicide terrorism.
Suffice it to say that there is no lack of
Islamic Web sites that provide media outlets
to terrorist organizations such as Al-Qaida.
Additionally, most news organizations as
well as leading news correspondents have
web sites and business/personal Internet
addresses which can be used as conduits to
funnel propaganda into the mainstream
media.

While propaganda spills into
supportive expatriate communities,
recruiting as a tool reaches throughout the
Web, coming to rest not only in Muslim
communities, but among all whom can
further the cause of terrorist organizations.

In one instance, Khalid Ibrahim, a
member of the Pakistani terrorist group
Harkat-Ul-Ansar, with suspected ties to Al-
Qaida, recruited online an 18- year-old
hacker named Chameleon from California.
As Mckay (1998) relates:

“I went to my post-office box one
morning, and there was US$1,000
with a number to call in Boston”,
said Chameleon. Chameleon, who
spoke to “Wired News” on the
condition of anonymity, said what
while he did cash the check from
Ibrahim, he considers himself a
computer enthusiast, not a terrorist.
Ibrahim was allegedly seeking maps
of US government computer
networks that Chameleon had
obtained on his travels through the
net. (p. 1)

Recruiting as a tool is aimed at both the
witting and unwitting, the money raiser, the
hacker, the possible terrorist. Any
organization, person, or tool, can be
exploited through Muslim ISPs for use in
netwar by Al-Qaida. This exploitation can
take many forms, such as the use of
surrogates to perform acts of netwar, or the
use of insiders to provide key information
that allows disruptions to take place. The
only tools needed to initiate a cyber attack –
computer, modem, telephone connection,
and user-friendly hacker software easily
downloaded from posted hacker sites, are
widely available.

INTELLIGENCE GATHERING

The ease of connecting to the net
through Muslim ISPs makes intelligence
gathering a foremost tool used by terrorist
organizations. Not only can terrorist
organizations gather information on stated
enemy national infrastructures and
personalities, the Internet allows monitoring
of how nation- states respond to cyber
attacks across the ICT spectrum, allowing
careful analysis of how best to exploit
weaknesses without being identified. The
plethora of Internet chat rooms where
hackers trade information and pass crack
code and other pirated software are prime
intelligence sites for terrorist organizations.
The very nature of the Web provides
anonymity at these sites, which in turn
provides security. Merkle writes that:

... anonymity and security factors are
both present on-line. You can curse
and scream and threaten with-
almost-total impunity. You can
speed away if you’re retaliated on by
another highway terrorist. You can
put a hurt on him yourself, as we’ve
seen. Cyber-road-rage. The
transformation is nothing short of
awesome. (p. 92)

This means that everyone you come into
contact with on the Web is a likely
intelligence source, recruit, or possible
surrogate, who can bring others with him to
accomplish the terrorist organization’s goals. By simply listening in on chat rooms, or reading online bulletin boards, the terrorist organization can discover individuals and cybergangs that can be wittingly and unwittingly recruited. Terrorist organizations can also find out what people know and the capabilities they possess. The capability for a terrorist organization to recruit across a wide spectrum, enlisting individuals and others for concentrated intelligence tasks or attacks, is a growing threat.

PERCEPTION MANAGEMENT

Perception management, which attempts to affect the perceptions of others in order to influence their emotions, reasoning, decisions, and ultimately their actions, is perhaps the most dangerous weapon in the hands of a cyberterrorist. It may take many forms, and can quickly reach mass audiences via the Internet. Denning relates that, “practically any speech act affects perceptions, so the possibilities for information warfare are endless” (p. 102). Denning goes on to relate:

The Internet is challenging television as a medium for reaching mass audiences and influencing opinion and decisions. Anyone can set up a Web site and control content on its pages. The cost is negligible, the potential audience huge. Like broadcast TV, the Internet also offers the ability to provide real-time audio and video. Laws and regulations may restrict what can be posted (as they do with TV and other media), but persons wishing to spread their message can do so without owning an expensive broadcast station or enticing an owner of one to carry their message. Consequently, the Internet is a great equalizer, giving individuals and small groups the same opportunities to be heard as governments and large corporations. (p. 102)

What makes the use of perception management over the Internet through Muslim ISPs unique is that the Internet can also be used as a destructive force in and of itself. For example, through use of Muslim ISPs via Islamic Web sites and email messaging, not only can a terrorist organization threaten a nation-state with some type of violent act, or the possible employment of Weapons of Mass Destruction (WMD), they can - at the same time - obstruct vital communications such as 911 responses through the same medium when and if the act is carried out. Terrorist organizations could obtain further leverage from a violent act by using Muslim ISPs’ to provide anonymous video and text over the Internet to news organizations, who would become unwitting conduits of this information and images to a national audience. Today’s digital technology makes it easy to fabricate or falsify information, or alter digital video in real time, even while the video is playing. Denning states that “anyone can be made to appear practically anywhere saying practically anything. The possibilities for deceit are endless” (p. 104).

The use of perception management can take many forms and is limited only to the imagination. In the skilled hands of a committed terrorist organization, the use of perception management is a lethal tool in their conduct of netwar.

OTHER REASONS TO USE MUSLIM ISPs

Reasons to use Muslim ISPs do not have to be as esoteric as those mentioned above. Even though a Muslim ISP can be started with moderate cash outlay, it still takes money to run. In a poor country such as Pakistan, outside sources of money may be the only thing keeping a particular ISP
from going under. By supporting Muslim ISPs’, terrorist organizations gain both a vehicle to spread their message and the goodwill that flows from the knowledge of their generosity. Location is another factor. Terrorist organizations stay out of reach of law enforcement and antiterrorism organizations by using Muslim ISPs’ in countries far removed from their intended target. They can operate freely in countries that have free speech laws, and can quickly move if their operations are threatened. Lastly, by using established Muslim ISPs’, terrorist organizations do not have to lay out substantial cash or risk exposure.

CONCLUSION
At the request of Caleb Temple, Defense Intelligence Agency, this paper has attempted to provide some explanations as to why Islamic terrorist organizations, including UBL’s Al-Qaida, would use established Muslim Internet Service Providers. These Muslim ISPs, which span the continents, provide secure, worldwide access to national audiences, as well as to small, radical terrorist elements committed to Jihad against “infidel” nation-states. Muslim ISPs provide covert, encrypted communication avenues, links to other terrorist groups and societies, and a forum to disseminate propaganda and manipulate perceptions on a world scale. By using Muslim ISPs, terrorist organizations can collect intelligence on enemy states and organizations, recruit witting and unwitting personnel, raise monies through front organizations, and leverage use and threatened use of Weapons of Mass Destruction. By using Muslim ISP networks, terrorist organizations have spread throughout the world, while staying out of reach of law enforcement agencies.

How do we combat Islamic terrorists’ use of Muslim ISPs? First, we must task assets to collect on Islamic and Muslim Web sites while identifying the Muslim, and non-Muslim ISPs that are hosting these sites. If we can identify organizations and individuals using these sites for terrorist activities, we can take steps to identify them, and if so desired, collect on them, or expose them publicly and/or privately through the targeted use of media or individuals.

Once Muslim ISPs allowing terrorist activities are identified, pressure can be brought to bear on Tier 1 and 2 telephony providers to cancel service, effectively bankrupting that ISP. This would send shock waves through the ISP community, forcing many to re-evaluate content allowed on their Web sites and through their telephony services. We can employ ‘black’ Internet activities such as code and/or program boobytraps, contamination, and counterfeits, deploying these into targeted Islamic and Muslim Web sites, throwing the terrorist and his organization off-balance and shaking their confidence. We can use ‘tagged’ codes and/or programs, which can be inserted into various web sites or attached to communications; then tracking these tags to identify links between Islamic terrorists and their evolving networks. We can surreptitiously host websites, chatrooms, and bulletin boards to identify and recruit suspected Islamic/Muslim terrorists/hackers. Once indoctrinated, they can be released to spread information and misinformation against their own terrorist networks.

As one can see, only the imagination, and existing national and international laws limit the avenues available to counter this growing ISP based threat. It is imperative that we recognize the implications of terrorist use of Muslim ISPs, and respond with appropriate countermeasures.
BIBLIOGRAPHY


