Section 3: Computer Viruses and Cyber Terrorism

Lecture Outline

1. Viruses and Malicious Code
2. Cyberterrorism

Viruses and Malicious Code

There is probably no area of computer crime that creates more fear, misperceptions, and attention than computer viruses

The market for virus protection software, firewalls, and computer security expertise is a multibillion dollar industry that relies on the same fears that drive many to purchase home security systems.

The market relies on two things to survive:

1. **Lack of knowledge**: Most people are not very savy when it comes to computers.
2. **Fear of Damage**: Media coverage has portrayed the damage from viruses as being biblical in nature.

- The financial damage from viruses has come largely from people believing the hype and rhetoric about viruses and willingly purchasing virus software they do not need in order to protect themselves.

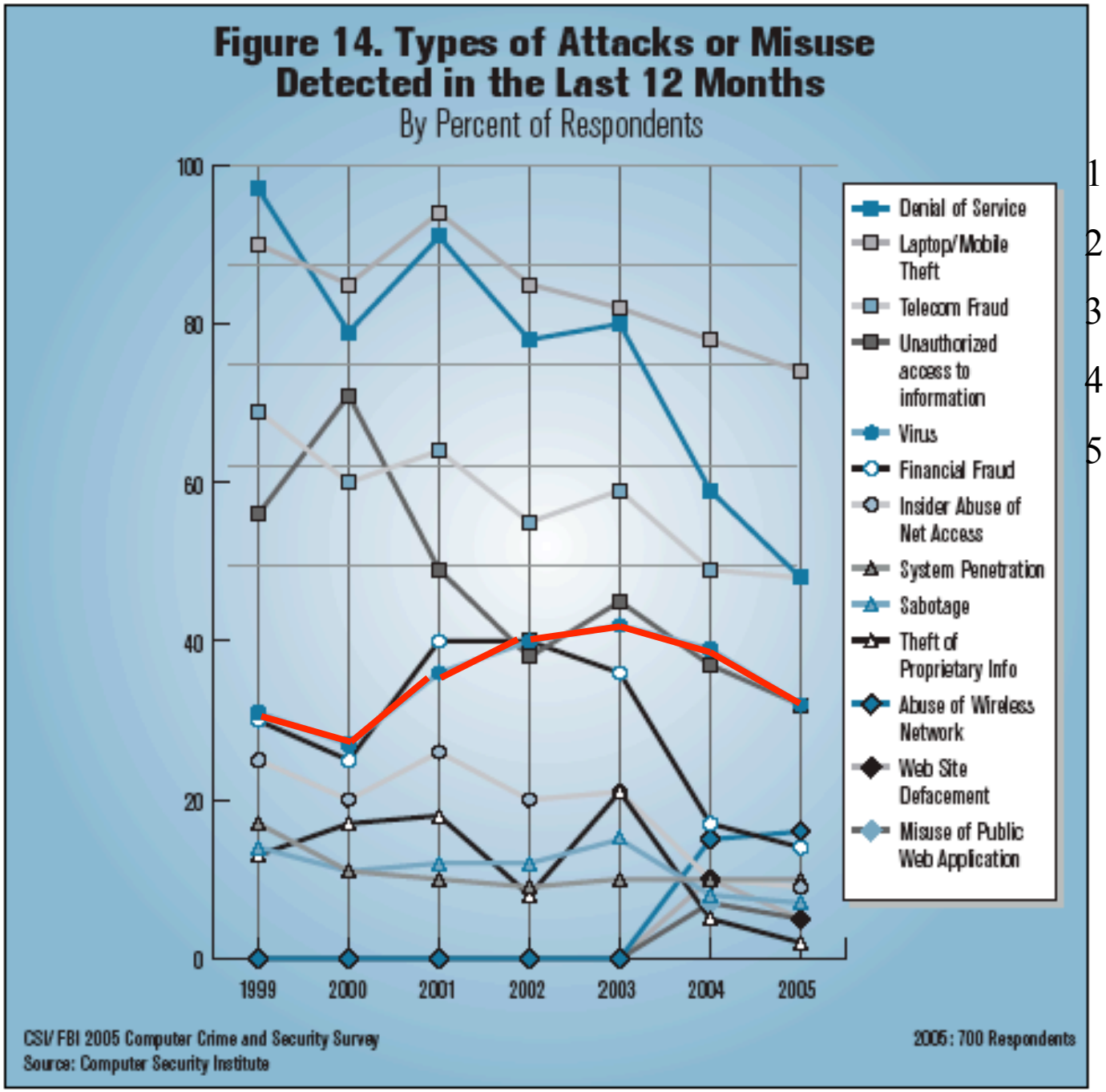
Viruses and Malicious Code

The true costs of viruses are unknown and incapable of being known because the damage that they create is often difficult or impossible to quantify accurately.

**This is not to make light of the problem, but rather to put it in perspective and give people a common sense grounding in the fact that much of the multibillion dollar loss figures from viruses come from the companies making multibillion dollar profits off of selling anti-virus software.

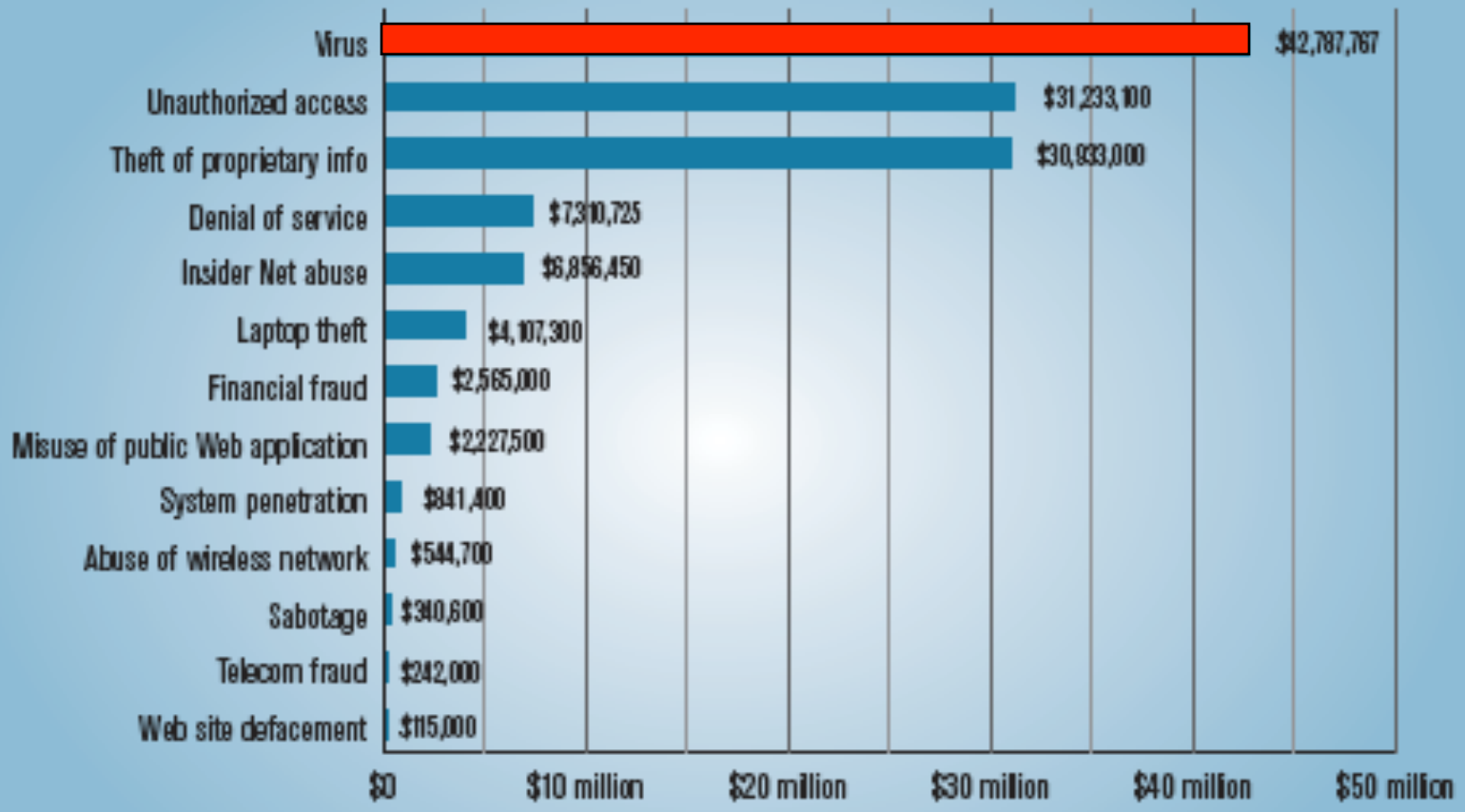
Extent of Problem

- No central database that collects information on damage that viruses cause.
- All data comes from surveys of government, private industry and universities.
- Data shows problem is decreasing over past few years.



1. Laptop/Mobile theft
2. DNS attack
3. Telecom fraud
4. Virus
5. Unauthorized access

Figure 16. Dollar Amount Losses by Type



Total Losses for 2005 were $130,104,542

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

2005: 639 Respondents

Purpose of this Section

***This section is not designed to provide you a step by step guide on viruses and malicious code.

This section is an overview of:

•Types of viruses

•Malicious code

•Security problems in general

I am not an expert on viruses and malicious code and I do not want to be portrayed as a “false authority” on the subject.

I am simply going to provide you with established information about these issues.

Viruses

Viruses have been around almost as long as computers have been around

The first viruses were created in the 1960's, although they were not called viruses, but rabbits.

These early viruses ran on mainframe computers and were almost always the result of pranks or mistakes by system administrators

Importantly, these viruses were local computer problems only, in that they did not spread across computer systems as modern viruses do, nor did they cause major damages.

The first modern virus appeared on PC's in the middle to late 1980's around the time that PC ownership started to grow dramatically.

Early Viruses

Early viruses were much less destructive then those that are around today.

Most were spread via floppy disks and did humorous things such as play a song or delete a single document.

Limited in damage because of how they spread

The first widely spread virus was “Brain”, created by two brothers from Pakistan that wanted to see the extent of software piracy in Pakistan.

Early viruses were simple to recognize, identify, and then eliminate using early versions of antivirus software.

First big change in viruses came when the virus writers began to encrypt the code within the viruses, thus making it much harder to identify and eliminate.

Modern Viruses

Modern viruses really started to take shape in the 1990's because of the confluence of several main things:

1. **Improved Coding**: Virus writers became much more sophisticated in how they wrote and encrypted viruses, making them much more difficult to identify and eliminate.

Virus creation tools also became readily available making it so that more and more people could create viruses easily.

VCL (Virus Creation Laboratory) was the first virus code construction toolset that allowed for easy experimentation and creation of viruses by those who are not technically very adept.

Made writing a virus accessible to the masses (sort of).

VCL page

Modern Viruses

2. **Internet Growth**: The growth of the Internet allowed for viruses to spread much more like an actual virus than in the past.

In the past, viruses had to be spread by "sneaker link" with viruses being passed by floppy disks.

3. **PC Growth**: Growth of cheap PC's that run on Windows allowed viruses a much bigger audience.

With the market dominance of Windows and their focus on selling in volume, it created a huge class of victims for virus writers

**If the OS market was more balanced viruses might be a smaller problem because of the need to specialize for each OS.

Virus Classification

Classifying viruses is difficult at best, because of the constant changing nature of viruses.

Types of classifications

1. **Environment they operate in**: File, boot, macro, network.
2. **OS they target**: Windows, OS X, Linux, UNIX
3. **Encryption used**: No encryption or sophisticated.
4. **Destructive Capacity**: Prank to complete system failure.

In addition to these classifications, there are a list of other malicious codes including:

Worms, Trojan horses, adware/spyware, logic bombs, DNS attacks, and blended attacks.

Virus Environments

Viruses operate in four primary environments:

1. **File Viruses**: Infect their targets either as a companion or through file system specific features known as link viruses.

They use a particular operating system to propagate and can infect virtually any type of executable file.

These viruses can overwrite the contents of a file destroying the original contents.

These viruses are fairly easy to detect and remove because of how they have to be written.

Virus Environments

2. **Boot Viruses**: The viruses affect the boot area of a computer system.

Boot viruses take over a computer upon booting up or rebooting of an operating system.

Often difficult to remove because they can remove or relocate original boot code.

3. **Macro Viruses**: Found in commonly used business software such as spreadsheets, documents, databases, and other common productivity software.

Macro viruses take advantage of macro software languages built into common systems of business software.

Often used to destroy all documents on a computer as it “spreads” to other files of the same types.

Virus Environments

4. **Network Viruses**: Attack networks or e-mail servers in order to spread themselves.

Main aspect of a network virus is its ability to transfer its code to a remote server or workstation on its own.

Of all virus types, this one has the best capability to replicate and transfer itself quickly across a wide range of computers.

Sometimes limited by OS they can run on.

Worms

What is it: Stand alone piece of code that copies itself from one computer to another.

**Key difference between this and standard viruses, is that they don't need another piece of software to attach themselves to as they are designed to replicate on their own.

Damage: Runs the gamut from annoying to serious international incident.

** First couple were successful because of how they played upon peoples insecurity in sending them through e-mail.

Requires that a user do something for them to become infected, such as opening an unknown file.

Example: Code Red worm spread to 250,000 computers in just 9 hours, but did little real financial damage.

Trojan Horses

What is it: Unauthorized program contained within a legitimate program that performs functions unknown, and usually unwanted, by the user.

These programs often masquerade as something desirable, such as a joke or picture forwarded through e-mail.

The hidden program usually waits for some computer event to occur, a date to be reached or some other type of trigger and then delivers its payload.

Doesn't replicate itself, but can cause serious damage to the computer

Damage: Ranges from nothing to stealing of millions of dollars, depending on who has access to what.

Examples: Hidden payload can give access to the virus writer, destroy files, or simply display a message.

Trojan Horses

Most popular and widely used is the Backdoor Sub Seven Trojan.

It is a series of integrated programs that allow a remote user to gain control over a computer.

Once installed and operating, attackers can run any number of attacks and program, with the additional ability to change settings on a computer or make it into a zombie.

- Restart the OS
- Reverse mouse buttons
- Record sounds from the microphone
- Record images from an attached camera

Generally spy on a user using their own computer and all of its peripherals.

Types of Trojan Horses

Remote Access Trojans: Most common type of TH. Allows offender to do anything on a computer that a normal user can do.

Password Sending Trojans: Attempt to steal all of the cached passwords and also look for other passwords entered on the users computer and then e-mailing it to the offenders address.

Offenders often use free e-mail programs like yahoo and hotmail

Keyloggers: These programs log the keystrokes of the victim an let the offender search for passwords or other sensitive data in the log file.

Destructive: Only function is to destroy and delete files. These programs can be set up to automatically delete core system files or anything else.

Can be activated remotely or set to delete at a specific time.

Types of Trojan Horses

Denial of Service Trojans: Allows offenders to overload websites and effectively shut them down due to too much traffic.

Variant: Mail Bomb: Aim is to infect as many machines as possible via e-mail addresses.

Proxy/Wingate Trojans: Turn the victims computer into a zombie which can be used by the offender or sold to others for sending spam, DNS attacks, etc..

Software Detection Killers: Designed to kill popular anti-virus software installed on victims computer.

Once the Anti-virus software is destroyed, offenders can control the computer completely.

Adware/Spyware

What are they: Programs that are downloaded from various sources that do various things depending on if it is adware or spyware.

Often installed as companion software with a legitimate piece of software.

Similar to a Trojan horse in that many people do not know about them and they are hidden on their computer and co-opting their computer use.

Adware: Mostly annoying, these programs can do many things such as:

- Change browser
- Redirect homepages
- Pop up ads

Spyware: Sends back information about the user to a marketer.

Information includes:

Computer hardware; software used; pages visited on internet

Although not technically a virus, for many computer users they have the same disruptive impact as a virus.

Adware/Spyware

Damage: There is not generally any physical or financial damage to the user from these two types of software.

- Annoying
- Right to privacy issues

Spyware typically takes advantage of EULA's that people don't read that allows them to install the software on the computer.

These agreements are written in such a way that it is virtually impossible to determine what the spyware will and won't do.

Moreover, what the data is used for is almost never disclosed to the user.

Removing spyware is so onerous a task that it often requires the entire HD to be scrubbed and OS to be re-installed because of how the spyware integrated itself into these programs.

Denial of Service Attacks

What is it: Attacks on websites of network systems that prevents legitimate users from using the systems.

A DNS attack sends phony requests to a server that host a website or a network, overloading it and preventing users from accessing the site or network.

Increasingly, DNS attacks are being conducted using "zombie" PC's.

Damage: Depends on the site and on the extent of the attack.

In 2000 a DNS attack was launched against Yahoo, E*Trade, Amazon, and eBay, completely taking down their sites for several hours.

Financial damage results from losing customers who cannot access the sites.

Blended Threats

What is it: Combine characteristics of viruses, worms, Trojan horses, and malicious code with server and internet vulnerabilities to initiate, transmit, and spread an attack.

Idea is that by using multiple methods and techniques, blended threats can rapidly spread and cause widespread damage.

These attacks are increasing in number as they prove more successful and more tools are created to make them easy to create and spread.

Currently, few anti-virus packages can handle these attacks

Example: Code Red Work

Spread to 300,000 computers within 24 hours

Worm only existed in the memory of the target system as opposed to all other viruses which required a replication to be made on a remote system to work.

Virus Hoaxes

What is it: These are not real viruses, but rather people sending out e-mails about supposed viruses and things on your computer that you need to delete.

Relies on the fact that people don't know much at all about their computers and that they will trust almost anyone if they think they are an authority.

In effect people are so conditioned to respond to virus's that they inadvertently harm their own computer thinking they are protecting it.

The end results is that these fake viruses result in people damaging their own computers dramatically.

Fake Virus Example

A soon to be X friend sent me the following info ... I followed the instructions and sure enough, there it was! Here's msg he sent me ...

"Virus is called jdbgmgr.exe and is not detected by Norton or McAfee. It sits quietly for about 14 days before damaging the system and passing on to all other people in your address book. You'll have it most likely have it as you're in my address book and I found it. I managed to catch it in time (see instructions below). You should therefore also be able to catch it in time if you act on instructions below NOW. I got them from someone the same way you are getting them from me now.

INSTRUCTIONS:

Go to start, find or search option, check C drive and all subfolders in the Files/Folders option, type the name jdbgmgr.exe, make sure to check C drive and all subfolders. I found it in my C drive. Click windows, then the system folder. Click find now. The virus has a Teddy Bear Icon w/the same name jdbgmgr.exe. DO NOT OPEN IT. Go to Edit (on the menu bar) and choose select all to highlight the file without opening it. Now go to File (on menu bar) and select delete. It will then be sent to the re-cycle bin. Go to recycle bin and delete it from there as well. If you have this virus, please pass this on to everyone in your address book as they will be infected as well.

Fake Virus Example

Jdbgmgr.exe is an actual program on windows that is the Microsoft Debugger Registrar for Java.

While this may or may not cause a lot of damage to your computer it is an example of a fake virus that has been very popular.

Other fake viruses could very easily take out your computer if you fell for them.

Signs of a Fake Virus

- Contains a message about a virus and preaches salvation by deletion.
- Usually have many words in CAPS and exclamation points.
- Urge the reader to alert everyone they know and forward the e-mail.
- Seek credibility by describing the virus in baseless technical jargon.
- Claim the source of the virus is Bad

Vmyths site

Cyberstalking

What is it: Although there is no universally accepted definition of cyberstalking, the term is used in this report to refer to the use of the Internet, e-mail, or other electronic communications devices to stalk another person.

Stalking generally involves harassing or threatening behavior that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property.

While there are problems defining what stalking is there are even bigger problems trying to determine how much cyberstalking actually occurs

How Much Cyberstalking

Numbers No one knows how much offline stalking occurs on a yearly basis and trying to determine cyberstalking numbers is even harder.

1999 Attorney General Report on Cyberstalking

4 Main sources of data cited in the report

1. Comparison of offline stalking with cyberstalking.
2. Anecdotal evidence from law enforcement.
3. ISP data on complaints.
4. Sexual victimization of college students survey.

Importantly, 7 years later this data is till the most cited on the subject.

Comparing Offline to Cyberstalking

- 1 in 12 women and 1 in 45 men is stalked sometime in their life
- 1% of women and .45% of men were stalked in the last 12 months.

"In the United States, there are currently more than 80 million adults and 10 million children with access to the Internet. Assuming the proportion of cyberstalking victims is even a fraction of the proportion of persons who have been the victims of offline stalking within the preceding 12 months, ***there may be potentially*** tens or even hundreds of thousands of victims of recent cyberstalking incidents in the United States."

"Although such a "back of the envelope" calculation is inherently uncertain and speculative (given that it rests on an assumption about very different populations), it does give a rough sense of the potential magnitude of the problem."

Anecdotal Data

“Anecdotal evidence from law enforcement agencies indicates that cyberstalking is a serious - and growing - problem. At the federal level, several dozen matters have been referred (usually by the FBI) to U.S. Attorney's Offices for possible action.”

“In addition, some local law enforcement agencies are beginning to see cases of cyberstalking. For example, the Los Angeles District Attorney's Office estimates that e-mail or other electronic communications were a factor in approximately 20 percent of the roughly 600 cases handled by its Stalking and Threat Assessment Unit. The chief of the Sex Crimes Unit in the Manhattan District Attorney's Office also estimates that about 20 percent of the cases handled by the unit involve cyberstalking.”

No discussion of whether cases involve cyberstalking IN ADDITION TO offline stalking, such as sending a threatening e-mail in addition to keying your car, or whether they are cyberstalking only cases.

Importantly, these are very big distinctions

This is data that is basically dramatic case data that has no real numbers to back it up. Of all of the kinds of data used in the report, this data is often the most powerful because it often involves heart wrenching details of life threatening incidents.

Unfortunately there is nothing to show that these cases are typical

ISP Complaint Data

This data involves complaints received by an Internet Service Provider that someone is harassing them or stalking them.

“ISPs also are receiving a growing number of complaints about harassing and threatening behavior online. One major ISP receives approximately 15 complaints per month of cyberstalking, in comparison to virtually no complaints of cyberstalking just one or two years ago.”

Considering ISPs have thousands and in many cases millions of subscribers these numbers are so low as to be embarrassing to have included.

Sexual Victimization of College Students Survey

“As part of a large study on sexual victimization of college women, researchers at the University of Cincinnati conducted a national telephone survey of 4,446 randomly selected women attending two- and four-year institutions of higher education.

The survey was conducted during the 1996-97 academic year. In this survey, a stalking incident was defined as a case in which a respondent answered positively when asked if someone had "repeatedly followed you, watched you, phoned, written, e-mailed, or communicated with you in other ways that seemed obsessive and made you afraid or concerned for your safety."

The study found that 581 women (13.1 percent) were stalked and reported a total of 696 stalking incidents; the latter figure exceeds the number of victims because 15 percent of the women experienced more than one case of stalking during the survey period.

Of these 696 stalking incidents, 166 (24.7 percent) involved e-mail. Thus, 25 percent of stalking incidents among college women could be classified as involving cyberstalking”

Key to this is involved cyberstalking, not completely cyberstalking, possibly a component

Forms of Cyberstalking

Cyberstalking takes many forms and can range from juvenile to seriously life threatening.

Unfortunately, the only cases that ever get publicized are those that are life threatening and they make up by far the fewest incidents.

- Threatening e-mail
- Doctored pictures of the victim posted to websites
- Bogus comments attributed to the victim in chat rooms
    - I want to be raped
    - I have done _____ in the past
- Threatening IM
- Cellphone calling and harassment

Protect yourself from Cyberstalking

1. Beware of sites such as Facebook and similar sites where people post all of their personal information on the website.

2. Don't post personal information

3. Check with your ISP/University about how to handle stalking incidents.

4. Get e-mail. And call information and report it to the police as soon as possible

5. Use call block, e-mail filtering, caller ID, etc..

6. Use common sense when talking with people.

**There is only so much you can prevent stalking. There has always been and will always be stalking.

New technology may actually help prevent more stalking rather than just facilitate it.

Cyberterrorism

- Propaganda
- Recruiting
- Training
- Fundraising
- Communication
- Targeting

Propaganda

- Terrorist groups such as Al Qaeda have used websites as a way to target potential supporters and sympathizers as well as the international community.
- Sites are not only official Al Qaeda sites but also sites maintained by group members and supporters.
- The *Center for Islamic Studies and Research* is the official media wing of Al Qaeda.
  - Sawt al-Jihad: Bi-monthly virtual magazine
  - Al Khansa: Online magazine for women of Jihad
- Hammas and others have childrens website with games, chat, and downloads to help spread the word of Jihad to young children.

Propaganda

Propaganda


مجلة الفاتح - العدد الثالث والتسعون - الصفحة الرئيسة
http://www.al-fateh.net/
Google
Financial
Personal Webpages
Apple
EKU
Yahoo!
EKU Webmail
GBP Mail - Login
Sports
News (12)
Tech Links
Cybercrime
Cyberterror
Urban Planning
Terrorist Groups
مجلة الفاتح
مجلة الفتيان والفتيات ... مجلة بناة المستقبل
الصفحة الرئيسية
أصدقاء الفاتح
الأعداد السابقة
مواقع أطفال
سجل الزوار
أخبر صديقك
اتصل بنا
محتويات العدد
وصايا علمية
تصدر في ١ و ١٥ من كل شهر
٢٠٠٧/٠٢/٠١
أطفال فلسطين
الأناشيد
الكمبيوتر
الألعاب
الألغاز
المسابقة
إبتسامات
مشاركات
الرسائل
بإمكانكم إضافة بريدكم الإلكتروني لنرسل إليكم التحديثات والإضافات
أرسل
مجلة الفاتح
أبرز الأحداث في الأراضي الفلسطينية
أناشيد مصورة : يا طيبة

Propaganda

Al Fateh: “The Conqueror”

Site includes games, chat, music, etc..

Sample pages of the site discuss Jihad and “unequalled tales of heroism”

October 2004, published a picture of a decapitated head of a female suicide bomber who had killed several Israeli soldiers

The accompanying text praises the act and states that she was now in paradise

2001 they posted the last will of a suicide bomber

Common Aspects of Propaganda

- Provide news articles w/fundamentalist spin
- Editorials and commentary from Islamic religious and military leaders
- Rulings on legal and religious matters
- Photos of alleged atrocities
- Links to other sympathizer sites
- Arabic only content

Recruitment

- In addition to using the web for propaganda, many of the terrorist web sites are also used for recruiting of would be Jihadis
- These sites often include numerous tools for recruiting individuals:
  - Bios on famous Mujahideen
  - Photos
  - Interviews with Jihadi in the field, battle accounts
  - Video footage
  - Poetry glorifying acts

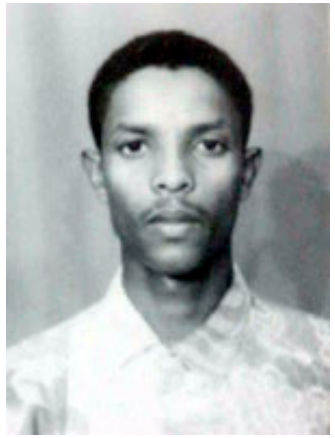
In many respects the videos shown are a lot like U.S. Military ads and the “Be all that you can be”, filmed and edited in the same style as western music videos

Recruitment

- One of the main techniques for recruiting is the use of message boards and chat rooms.
- Recruiting on this level is done by skilled individuals who know how to draw recruits into the movement.
- Here terrorist groups seek out specific types of recruits
  - Start a chat
  - Discuss their background: Looking for educated recruits
  - Provide videos and pictures to aid in conversion
- Almost like a religious conversion in the warmth and compassion used to recruit certain types of people.

- Forums have become moderated recently as more pro-Americans have infiltrated the chats in order to take them down.

Recruitment Example



Fazul Abdullah Mohammed, a.k.a “Haroun Fazul”

•One of the FBI’s Most Wanted Terrorist

•Reportedly very good with computers

•In testimony his wife is quoted as saying “he had a job in the Sudan working on computers”.

•Educated in Pakistan madrassa and selected for training at AQ’s Afghani training camps

•Returned to Africa to work as a covert operations leader

•Cover was that of a computer engineering student and then a computer worker.

•Indicted as mastermind behind the 1998 U.S. Embassy bombing in Nairobi Kenya.

Training

- The Internet has become a great source of training for terrorists for several reasons
- **Open nature of the Internet**: Information is everywhere and largely uncensored.
  - Almost anything can be found on the Internet using Google.
- **Easy Dissemination**: Allows for easy dissemination of ideas, training practices, and methods anonymously and covertly using numerous different methods.
- **Purchasing**: Almost any kind of training manual ever printed can be purchased online.
- **Multi-media**: Rather than just download books and .pdf guides, the Internet allows for full motion video and detailed audio and photos of techniques not easily learned by reading alone.

Known Training Guides

- Video
  - Creating suicide belt,
  - Manufacturing roadside bombs
  - Improvised ED's
- Downloadable manuals
  - Terrorist's Handbook
  - Anarchists cookbook
  - Poison manuals
  - Encyclopedia of Jihad
- Bi-monthly newsletters
  - Al Battar "Sword of the Prophets"
- Al Qaeda and others have been extremely effective at producing and disseminating training and handbooks to cells and groups worldwide.

Encyclopedia of Jihad

Found by the NY Times reporters in 2002 in Pakistan

Contains 10 or 11 chapters of “essential knowledge”

- Making explosives
- First Aid
- Use of pistols, grenades, and mines
- Espionage and reconnaissance
- Security precautions
- History and design of tanks
- Physical fitness

Training

Al Battar “Sword of the Prophets”

Al Qaeda bi-monthly training magazine

Al Battar Issue 20

- Assess U.S. security 3 years after 9/11
- Detailed instructions on developing secure plans for missions
- Detailed instructions on secure meetings and operational planning

Training

Overall the Internet has been an excellent source of training information for Terrorist groups

- Incredible source of information
- Anonymous and hard to remove training materials completely.
- Multimedia content is created and distributed allowing great detail.
- Cheap and easy to produce and distribute.

Information valuable to terrorist will always be available to terrorists on the Internet no matter how it is regulated.

Fundraising

- Like all other political groups, Terrorist organizations have found the Internet an excellent source of fundraising
- Some of the most basic methods that have been used have involved using the internet to ask for donations
- Posting bank accounts for donations
  - Groups place bank accounts on websites with pleas for money.
  - These accounts are difficult to trace and eliminate
- Non-Government Organizations
  - Fake NGO's are created and used to launder money
- Sales of Goods on Terrorist group sites
  - Some groups sell trinkets and goods to raise money, like an Internet bake sale

Fundraising-Pleas for Donations

Postings on chat sites and semi-legitimate news sites that ask for money and list bank accounts to donate to.

Fundraising-Credit card Fraud

A reporter for the Christian Science Monitor had his credit card number stolen while eating at a restaurant in Amman Jordan.

Although he never lost his card or any of his receipts, his credit card was used to purchase a Russian made night-vision rifle scope and a U.S. made range finder.

The goods were shipped to an address in Saudi Arabia.

Another colleague also had purchases made to their credit card shipped to the same address. They had also eaten at the same restaurant.

While these incidents are small scale, it is evidence of a larger problem with small scale financing.

Fundraising-Credit Card Fraud

Found on a Al Qaeda site along with instructions on how to download and use the program

Fundraising

Like all other political groups, Terrorist organizations have found the Internet an excellent source of fundraising

- Posting bank accounts for donations
- Solicitations based on demographics
- Non-Government Organizations
- "Charities"
  - Benevolence International Foundation
  - Global Relief Foundation
- Sales of Goods
- Cybercrime
  - Credit Card fraud
  - Phishing scams
  - Organized crime

Communication

- Anonymity, speed, cost and global reach of the internet has allowed terrorists to communicate within and between groups more easily.
- Through the use of the internet, geographically dispersed but ideologically similar groups are able to network and share tactics, planning, and technology.
- Surveillance is increasingly difficult due to anonymity and dispersed nature of the technology involved.
  - Free and anonymous e-mail
  - Web sites and chat rooms
  - Steganography
  - Cryptography

Communication

In January 2002 the Wall Street Journal acquired 2 computers from a looter in Kabul.

The computers were allegedly abandoned as the Taliban moved out of Kabul

On the computers they found:

•1,750 + text and video files, most of them encrypted

•A file containing 170 names of Al Qaeda members

•Report on planned operation to “gather intelligence about American soldiers”

•Primer on coding and encryption of documents.

•Procedures for transmitting messages via Pakistan

Communication-Steganography

Steganography

The diagram on the left is embedded in the picture on the right.

http://www.garykessler.net/library/fsc_stego.html

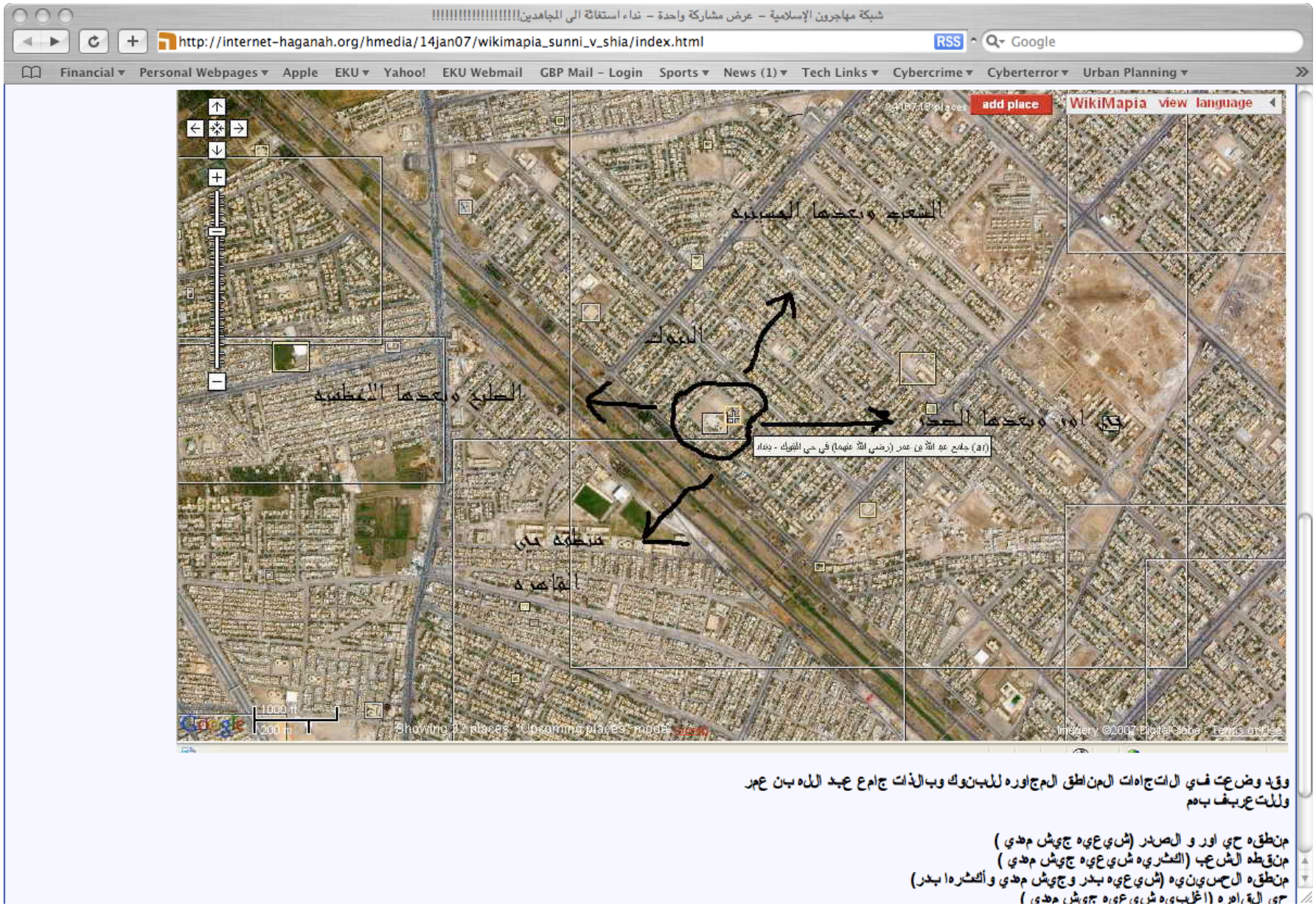
Target Information Packages

- According to testimony before the Senate Committee on Foreign Relations' Subcommittee on International Operations and Terrorism in 2001, targeting by terrorist groups have become much more sophisticated.
- Prior to carrying out an operation, Al Qaeda conducts surveillance of the target, often on multiple occasions.
- Use locals for surveillance and enter location without suspicion.
- Create elaborate "ops plans" or targeting plans
  - Photographs
  - CADCAM
  - Operative notes

Target Information Gathering

- Company databases online
  - Wireless network specifications
  - Personnel lists
  - Description of backup facilities
- Blueprints and building layouts
  - Floor plans
  - Ventilation ductwork
- Google Earth
  - Enhanced imagery and map combination

Targeting


http://internet-haganah.org/hmedia/14jan07/wikimapia_sunni_v_shia/index.html
add place
WikiMapia
view
language
الشعب وبعدها المسبيه
البيوك
الطلح وبعدها المطيبه
الصدر
Showing 32 places "Upcoming places" mode
Imagery ©2007 DigitalGlobe

Targeting


© 2007 Europa Technologies
© 2007 Sanborn
Image © 2007 Sanborn
Google
Pointer 38°53'43.47" N 77°02'06.78" W elev 6 m
Streaming 100%
Eye alt 2.64 km

Targeting


© 2007 Europa Technologies
© 2007 Sanborn
Image © 2007 Sanborn
Google
Pointer 38°53'43.09" N 77°02'06.90" W elev 5 m
Streaming 100%
Eye alt 734 m

Targeting


© 2007 Europa Technologies
© 2007 Sanborn
Image © 2007 Sanborn
©2006 Google
Pointer 38°53'38.63" N 77°02'13.56" W elev 3 m
Streaming 100%
Eye alt 55 m

End section 3