Slide 1

Examining the Cyber Capabilities of Islamic Terrorist Groups

Technical Analysis Group
November 2003

Institute for Security Technology Studies at Dartmouth College

Please address comments or questions to:
Technical Analysis Group
Institute for Security Technology Studies
45 Lyme Road
Hanover, NH 03755
Telephone: (603) 646-0700
Fax: (603) 646-0660
Email: itb@ists.dartmouth.edu

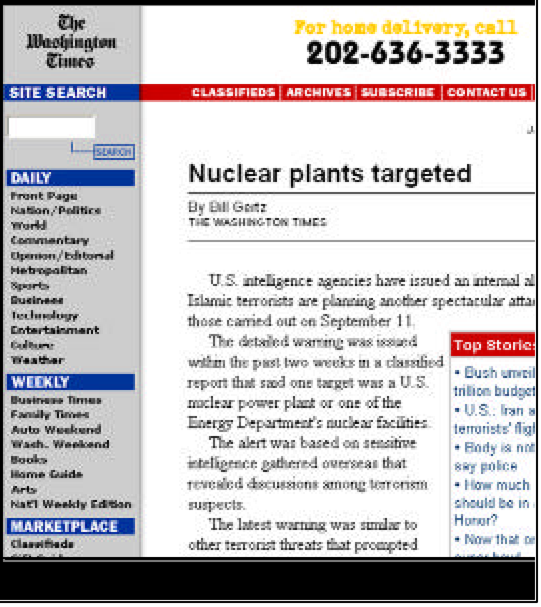
This project was supported under Award No. 2000-DT-CX-K001 from the Office for Domestic Preparedness, U.S. Department of Homeland Security

Points of view in this document are those of the authors and do not necessarily represent the official position of Dartmouth College or the U.S. Department of Homeland Security

Slide 2

Terrorism: Background

- The threat of terrorist attacks against U.S. citizens and U.S. interests around the world has become the Nation's principal security issue
- The cyber security of the United States is of paramount importance



The Washington Times

For home delivery, call
202-636-3333

SITE SEARCH

CLASSIFIEDS | ARCHIVES | SUBSCRIBE | CONTACT US

SEARCH

DAILY
Front Page
Nation/Politics
World
Commentary
Opinion/Editorial
Metropolitan
Sports
Business
Technology
Entertainment
Culture
Weather

WEEKLY
Business Times
Family Times
Auto Weekend
Wash. Weekend
Books
Home Guide
Arts
Nat'l Weekly Edition

MARKETPLACE
Classifieds

Nuclear plants targeted

By Bill Gertz
THE WASHINGTON TIMES

U.S. intelligence agencies have issued an internal al
Islamic terrorists are planning another spectacular atta
those carried out on September 11.

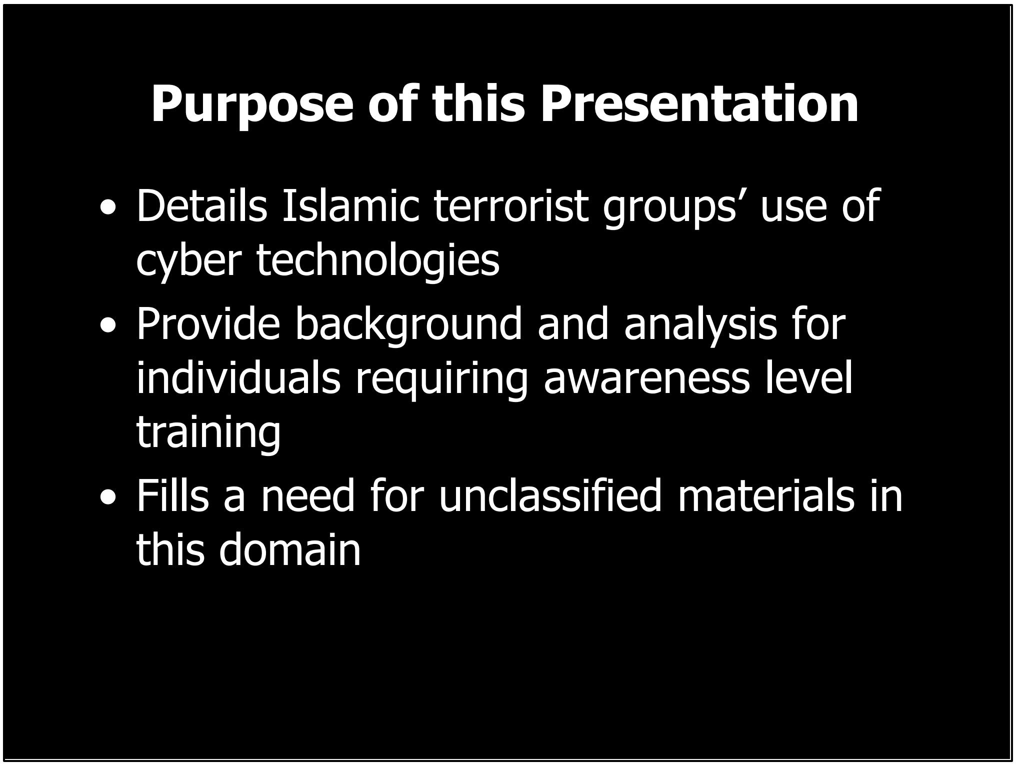
The detailed warning was issued within the past two weeks in a classified report that said one target was a U.S. nuclear power plant or one of the Energy Department's nuclear facilities.

The alert was based on sensitive intelligence gathered overseas that revealed discussions among terrorism suspects.

The latest warning was similar to other terrorist threats that prompted

Top Storie
- Bush unveil trillion budget
- U.S.: Iran a terrorists' fligl
- Body is not say police
- How much should be in Honor?
- Now that o

Slide 3



Purpose of this Presentation

- Details Islamic terrorist groups’ use of cyber technologies
- Provide background and analysis for individuals requiring awareness level training
- Fills a need for unclassified materials in this domain

Islamic terrorist groups have used combinations of ancient guerrilla warfare tactics and advanced technologies to carry out their goals. They have shown themselves to be practitioners of unconventional warfare by staging operations around the globe against high-visibility, high-value targets, using very small teams, producing dramatic results with relatively little expenditure, all without ever engaging in direct battlefield attacks against an opposing military force.

While there has been much discussion in the public realm regarding terrorist groups’ use of centuries-old means of communications (use of human couriers) and financial transactions (such as “hawallah” a form of unlicensed money transfer business) to avoid detection in their operations by global intelligence services, there are clear indications that terrorist groups are willing to use and manipulate the conveniences of Western technology when it makes sense for them to do so. Discussions in the public arena between law enforcement and terrorism investigators and the private sector revealed that there is a lack of authoritative unclassified materials concerning the use of cyber technology by Islamic terrorist groups.

This briefing is the result of research specifically designed to meet this need. Examining the Cyber Capabilities of Islamic Terrorist Groups details how cyber technologies are exploited by these hostile entities. The open source materials used in this report include court testimony, indictments, government reports, academic reports, actual information from websites associated with terrorist groups (both from the organization itself and from sympathizer and affiliated groups), Congressional testimony, and the open media. This document uses these materials to present a clear picture for those who require awareness-level training in this domain, and provides a starting point for further research and analysis.

*** There are multiple spellings of the anglicized versions of the Arabic names and terms used throughout this presentation. We have made a best effort to choose a commonly accepted version of any word used more than once in the presentation and use that version consistently throughout. If a direct quotation uses a spelling different from the one we have chosen, we have used the spelling as given in the quotation.

Slide 4

New War - New Tactics

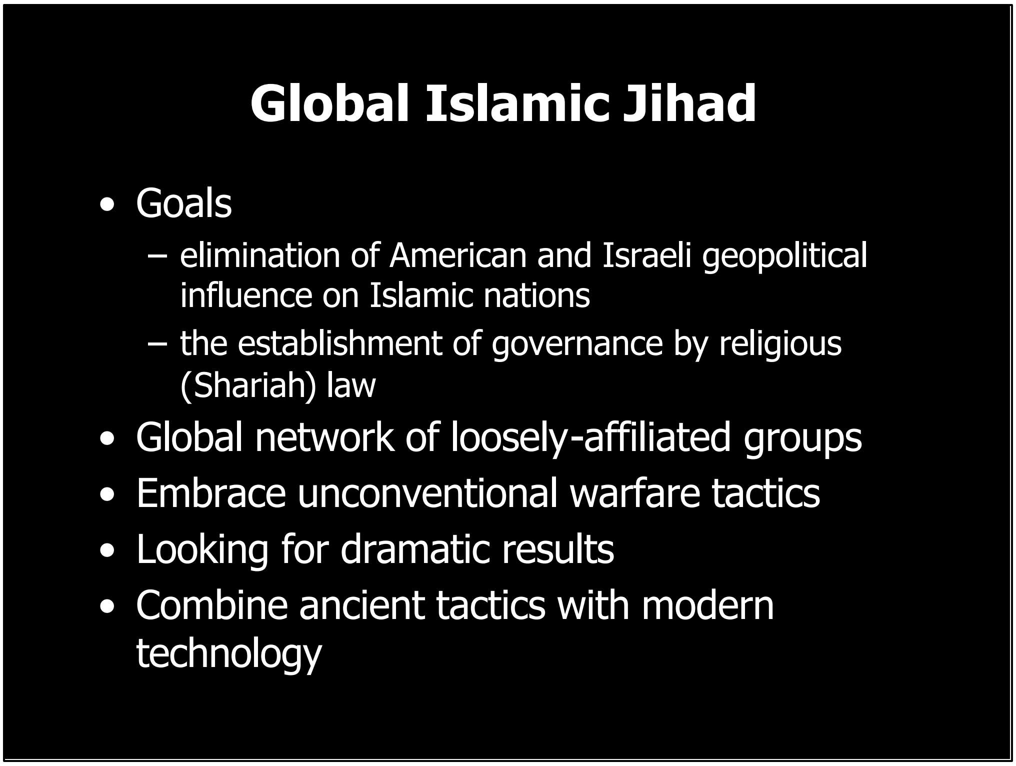
Cells from hell
AFGHANISTAN

Image Source: http://www.usnews.com/usnews/news/terror/graphics/cellsofhellmap.pdf

The global "War on Terrorism" is very different from wars fought in the past. Allies in this war are fighting against enemies who are in many cases without a nation state. These new enemies are seeking not to protect their homelands, but to overthrow existing governments and (in many cases) to establish radical new government and even new nation states. Because elements of this enemy are spread across the globe, united primarily by broad Islamist ideology but with localized agendas, the U.S. and its allies must strive to understand the very different ways that these groups are organizing and acting.

*** Nation State is defined for this report as a political organization where relatively homogenous people occupy sovereign territory.

Slide 5



Global Islamic Jihad

- Goals
  - elimination of American and Israeli geopolitical influence on Islamic nations
  - the establishment of governance by religious (Shariah) law
- Global network of loosely-affiliated groups
- Embrace unconventional warfare tactics
- Looking for dramatic results
- Combine ancient tactics with modern technology

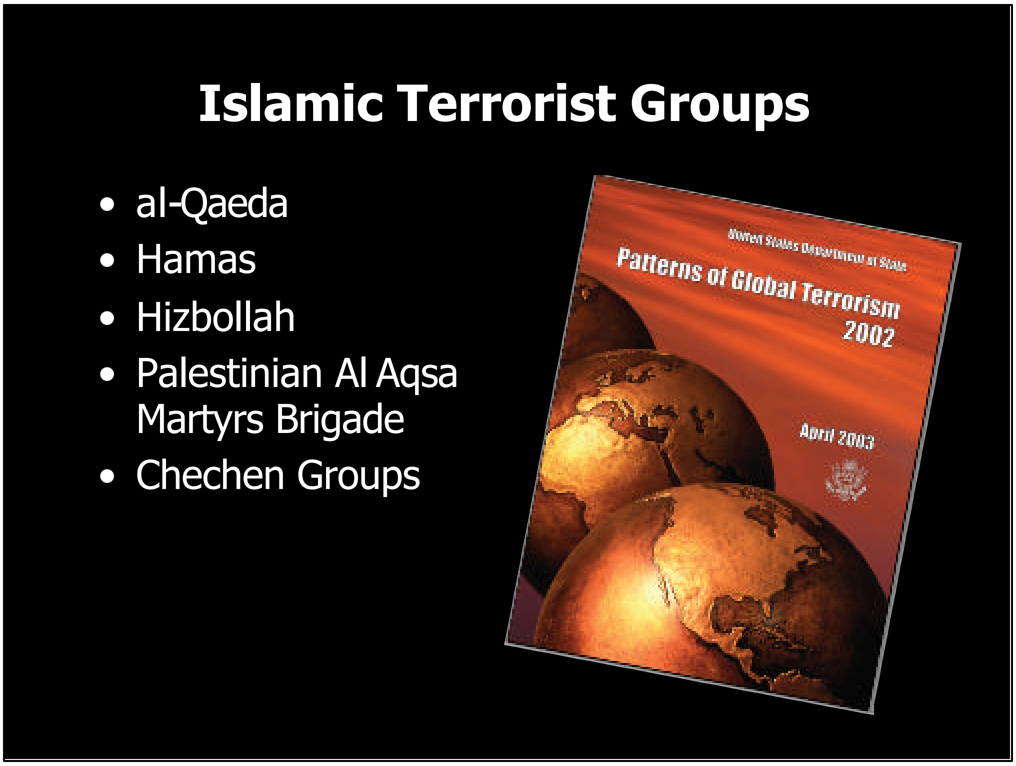
Although the War on Terrorism is not explicitly restricted to Islamic terrorism alone, Islamic terrorism is arguably the greatest current direct threat to our national security. The terrorist groups that collectively constitute the global Islamic jihad want the reduction or elimination of Israeli and American geopolitical influence on Islamic nations and (in many cases) the establishment of governance by Shariah law (a strict interpretation of Islamic religious law).

Separate Islamic fundamentalist terrorist groups have become in many ways a loose, global network of terrorist entities. These entities sometimes work together and sometimes in isolation. They embrace the concept of asymmetric warfare: the use of unconventional tactics to counter overwhelming conventional military superiority. The hallmarks of their operations are surprise, scale, and drama. They use both human couriers and encrypted satellite phones. Further, the C.I.A has already identified two known Islamic terrorist organizations, Hizballah and HAMAS, with the capability and greatest likelihood to use cyber attacks against our infrastructures.

<http://www.cbsnews.com/stories/2003/02/12/attack/main540283.shtml>

Testimony of John A. Serabian, CIA Information Operations Issue Manager before the Joint Congressional Economic Committee, February 30, 2000.
<http://www.cia.gov/cia/public_affairs/speeches/archives/2000/cyberthreats_022300.html>

Slide 6



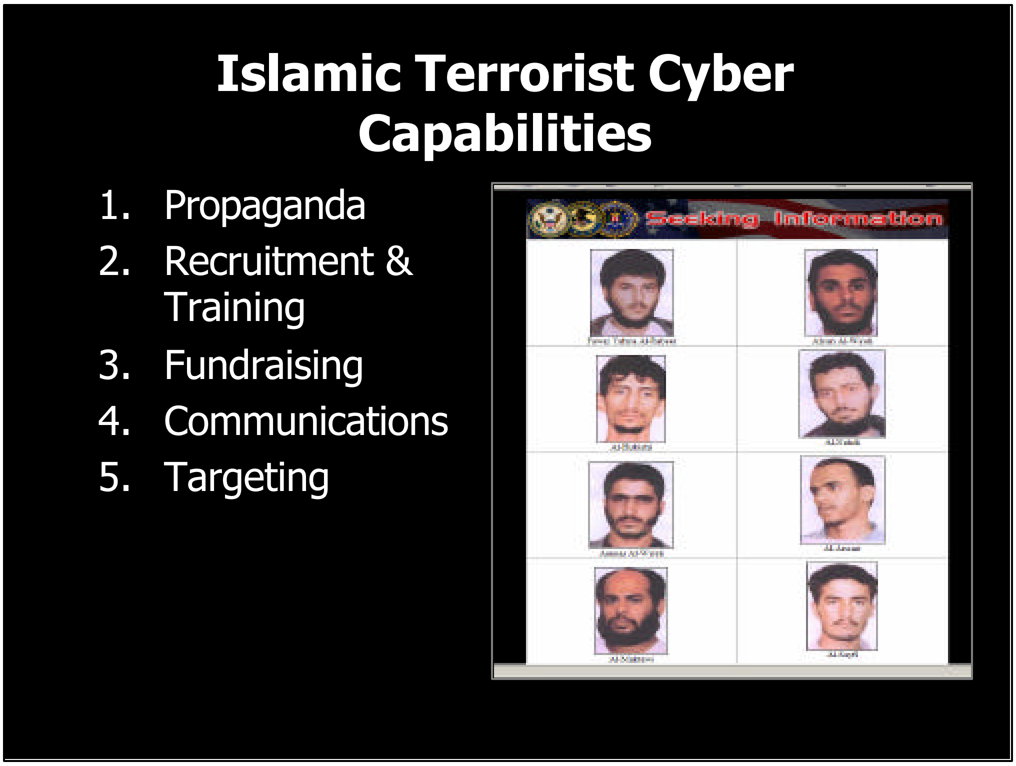
Islamic Terrorist Groups

- al-Qaeda
- Hamas
- Hizbollah
- Palestinian Al Aqsa Martyrs Brigade
- Chechen Groups

United States Department of State
Patterns of Global Terrorism 2002
April 2003

Examples of Islamic terrorist groups and descriptions of their activities may be found in the State Department's annual Patterns of Global Terrorism report is submitted in compliance with Title 22 of the United States Code, Section 2656f(a). This law requires the Department of State to provide Congress a full and complete annual report on terrorism for those countries and groups meeting the criteria of Section (a)(1) and (2) of the Act. This presentation cites examples from groups such as al-Qaeda, Hamas, Hizbollah, Palestinian Al Aqsa Martyrs Brigade, and Chechen Groups.

The Patterns of Global Terrorism report is available at the State Department's website <http://www.state.gov/s/ct/rls/pgtrpt/>.



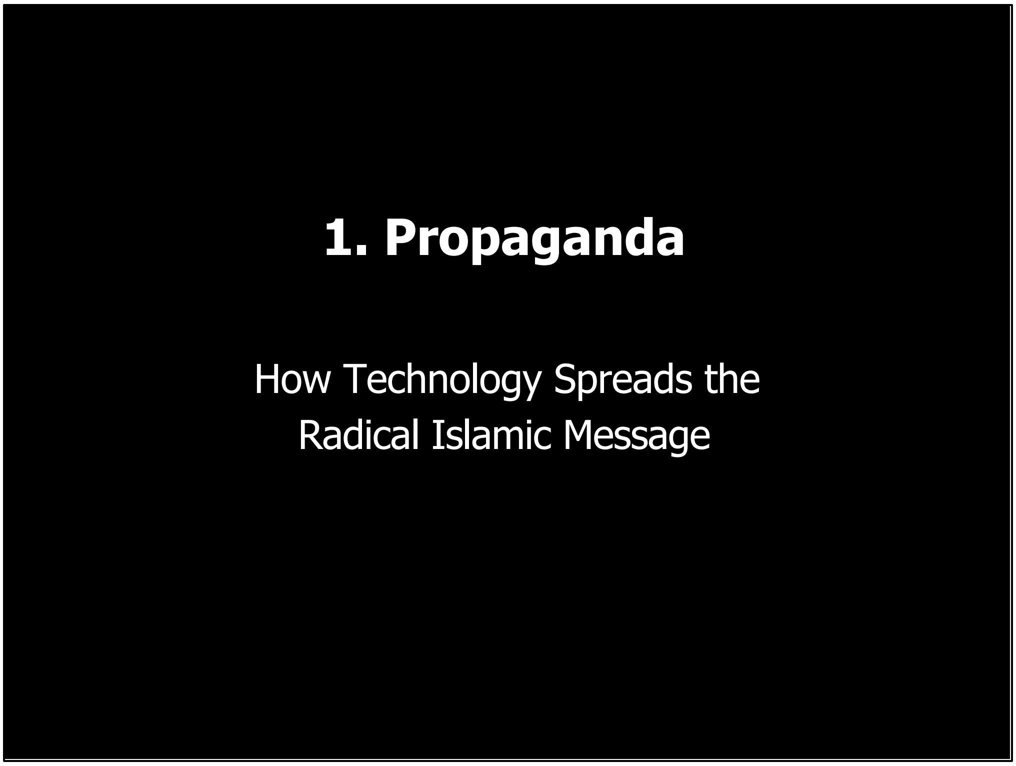
Islamic Terrorist Cyber Capabilities

1. Propaganda
2. Recruitment & Training
3. Fundraising
4. Communications
5. Targeting

The authors of this report have found five areas where there is clear, factual evidence that Islamic terrorism is flexing its muscles in the cyber realm. These areas are:

1. Propaganda
2. Recruitment & Training
3. Fundraising
4. Communications
5. Targeting

The following slides provide examples and analysis for each area.

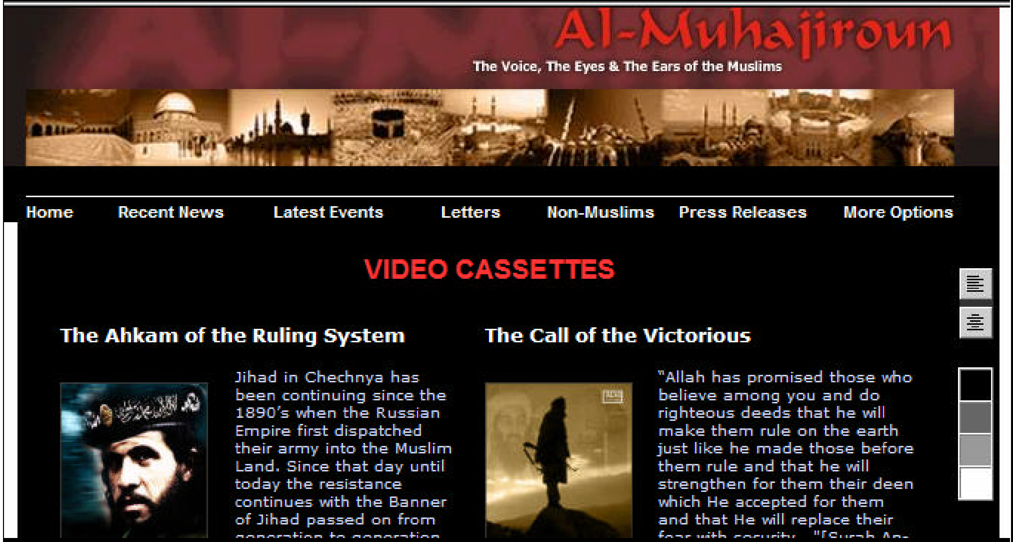


1. Propaganda

How Technology Spreads the
Radical Islamic Message

Slide 9

Getting their Attention



VIDEO CASSETTES

The Ahkam of the Ruling System

Jihad in Chechnya has been continuing since the 1890's when the Russian Empire first dispatched their army into the Muslim Land. Since that day until today the resistance continues with the Banner of Jihad passed on from generation to generation

The Call of the Victorious

"Allah has promised those who believe among you and do righteous deeds that he will make them rule on the earth just like he made those before them rule and that he will strengthen for them their deen which He accepted for them and that He will replace their fear with security. "[Surah An-

The cycle of engagement in a ideology-driven cause begins with getting the attention of like-minded individuals. This is often accomplished by broad campaigns of propaganda and possibly disinformation, often leveraging the involvement of third parties who are sympathetic to, if not directly involved in, the organization's cause. Islamic terrorists have clearly embraced this approach, and use Internet communications to pique interest and draw supporters in. They claim to speak for the masses, and in doing so also lay claim to impossible levels of popular support. The use of the Internet to spread propaganda speaks to the terrorists' and sympathizers' desire to target certain audiences, such as the educated but disenfranchised and the intelligentsia in Islamic countries, and the well-educated expatriates residing in Western countries.

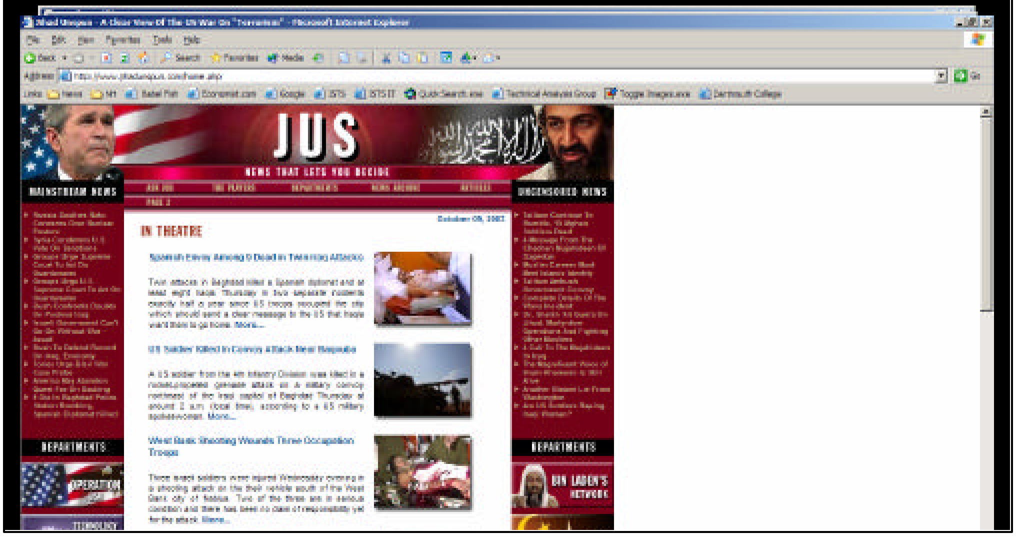
*** NOTE: It is possible that legitimate religious groups and web-sites may be included in the general description of terrorist propaganda and websites we analyzed. Given that terrorist sites may attempt to disguise themselves as "legitimate" religious groups, we do not attempt to distinguish which sites may be legitimate or contain some legitimate content.

Slide 10

Propaganda: Examples

www.jihadunspun.com

Rumored to be run by U.S. intelligence


Jihad Unspun - A Clear View Of The US War On "Terrorism" - Microsoft Internet Explorer
JUS
NEWS THAT LETS YOU DECIDE
MAINSTREAM NEWS
UNCENSORED NEWS
IN THEATRE
DEPARTMENTS
OPERATION
BIN LADEN'S NETWORK

Spanish Envoy Among 8 Dead In Twin Iraq Attacks

US Soldier Killed In Convoy Attack Near Baquoba

West Bank Shooting Wounds Three Occupation Troops

It is very clear that Islamic terrorists and their sympathizers make extensive use of the Internet to disseminate propaganda. Islamic fundamentalist websites are far too numerous to list comprehensively, but a very small sampling of some of the most active and well-known includes:

<http://www.kataebalaqsa.org> – Palestinian Al Aqsa Martyrs Brigade

<http://www.alneda.com> – primary al-Qaeda site hacked by U.S. groups as seen on this slide

<http://www.palestine-info.com> – The multi-lingual Hamas web site

And <http://www.jihadunspun.com> – controversial in jihadi circles, some say it is really run by the U.S. Intelligence community

Some of these sites include notations w/links to partial or full mirror sites (example: the Supporters of Shariah website - run under the direction of Omar Bakri al-Masry, religious leader of London's notorious Finsbury Park Mosque - is partially mirrored at <http://www.angelfire.com/dc/beghnet01/frame1.html> and other sites), recognizing that they are frequently subject to shutdown by ISPs or electronic attacks from those who do not agree with them. Virtually all of these fundamentalist sites have links to many other sites with similar or related viewpoints around the world, as well as very public media resources such as al-Jazeera, CNN, and the BBC. Interestingly, these sites fairly frequently also re-post "news" items and opinion pieces from American conspiracy-theorist websites, particularly ones w/a strongly anti-Semitic flavor.

The network of fundamentalist sites sharing news and information is vast. In many regards, the network of Islamist sites mirrors the amorphous organization of the global Islamic jihad concept. As in its physical structure, the Islamic terrorist web presence encompasses a wide range of direct and indirect connections, with some sites directly attributable to the highest levels of leadership while others are favorably inclined brother entities w/specific geographic agendas, right down to lone individuals who might at best be termed "fans" of organized terrorism.

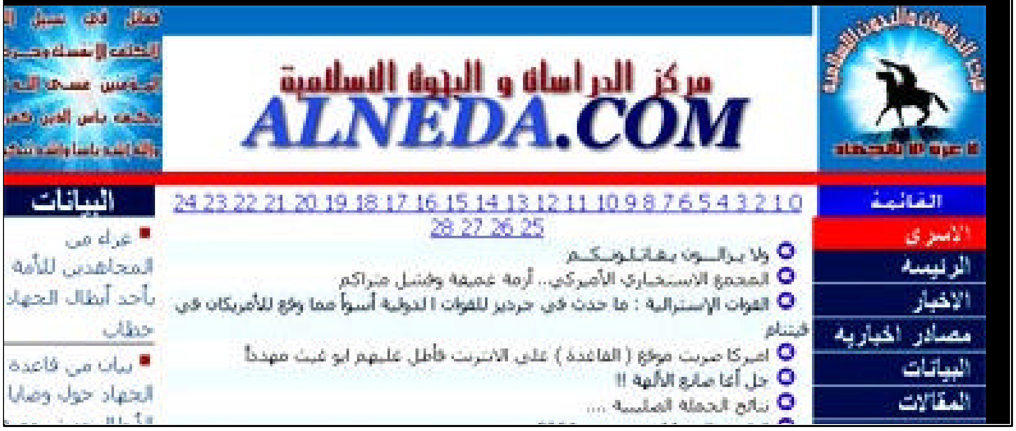
Of note: since this research was completed earlier this year (2003), a substantial number of these web sites have moved to new web addresses.

Testimony of Federal Bureau of Investigation Director Louis Freeh, Senate Select Committee on Intelligence, May 10, 2001. <http://www.fbi.gov/congress/congress01/freeh051001.htm>

Slide 11

Propaganda: Examples

- Main site associated with AQ: “Alneda” or the Calling
  - Releases AQ-attributed statements, rulings, and declarations
  - July 2002: No longer under www.alneda.com domain
  - February 2003: “parasiting” onto other legitimate sites



مركز الدراسات و البحوث الإسلامية

ALNEDA.COM

القائمة

الأسرى

الرئيسية

الأخبار

مصادر اخباريه

البيانات

المقالات

24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
28 27 26 25

○ ولا يزالون يقاتلونكم

○ المجمع الاستخباري الأمريكي.. أزمة عميقة وفشل متراكم

○ القوات الإسترالية : ما حدث في جرذير للقوات الدولية أسوأ مما وقع للأمريكان في فيتنام

○ امريكا ضربت موقع (القاعدة) على الانترنت فأطل عليهم ابو غيث مهدداً

○ حل أغا صانع الآلهة !!

○ نتائج الحملة الصليبية ....

البيانات

■ نعي من المجاهدين للأمة بأحد أبطال الجهاد خطاب

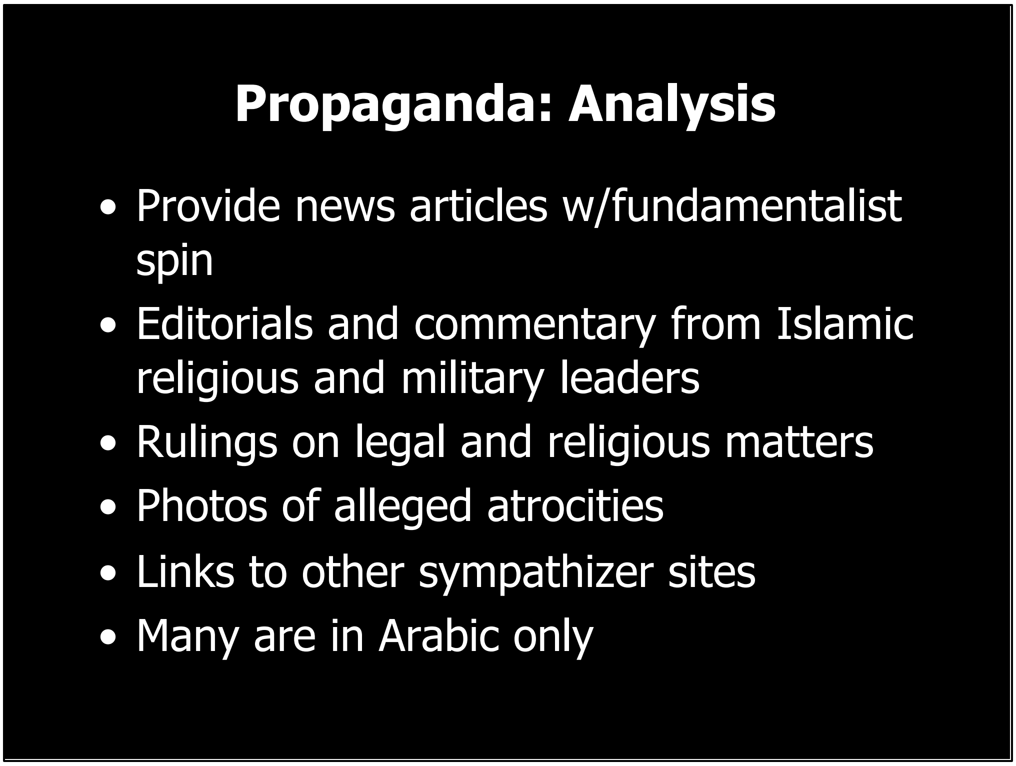
■ بيان من قاعدة الجهاد حول وصايا

One of the websites most consistently identified with al-Qaeda has been the Alneda site, which means – roughly – “the call” or “the calling”*. It was run under the auspices of an entity calling itself the Islamic Studies and Research Center, which is really a communications group within al-Qaeda or a joint effort between al-Qaeda and the Taliban. The site is extremely text-heavy. Through early 2003, this site was consistently one of the primary outlets of “official” statements from senior members of al-Qaeda, including bin Laden, Ayman al-Zawahiri (UBL’s right hand), and Sulemein Abu Gaith (the “official” AQ spokesman). It was on this site that al-Qaeda appears to have first directly claimed responsibility for the nightclub bombing in Bali, the attacks in Mombasa on an Israeli hotel and an Israeli commercial airliner, and the attack on the U.S.S. Cole, among other operations.

The dogged persistence with which this particular site has been perpetuated, retaining the same look, structure, and style of rhetoric – despite being thrown off from various web hosting services and being hacked by pro-American activists and hackers time and time again – strongly suggests that this has been an authentic outlet for al-Qaeda. There have also been reports in the media that U.S. intelligence professionals believe that this site (and others) may be used to transmit secret messages to al-Qaeda operatives, either through coded messages, encrypted file-sharing, password-protected areas of the site, or possibly even steganographic message transmission.

Since the summer of 2002, this site has not operated under its original domain (www.alneda.com). It has been kept alive by a technique of “parasiting” itself onto apparently unknowing legitimate domains, with its keepers burying its file structure deep in seemingly innocuous subdirectories of the legitimate site. Because this information resource existed only in cyberspace, it was ideally suited to AQ’s post-Afghanistan operational needs. Once AQ was largely deprived of the base of operations that Afghanistan previously provided, members scattered around the globe. Al-Qaeda’s use of the internet through web sites, email, message boards, and chat rooms allows dispersed members to stay in touch constantly, while maintaining the operational security and compartmentalization demanded by their work, under cover of the Net’s anonymity. Sidenote: there is an elite group of troops in Iraq (formerly under the command of one of Sadaam Hussein’s sons – Uday), charged w/ special operations including – reportedly – information operations, which is called al-Nida, also meaning “the calling”.

Slide 12



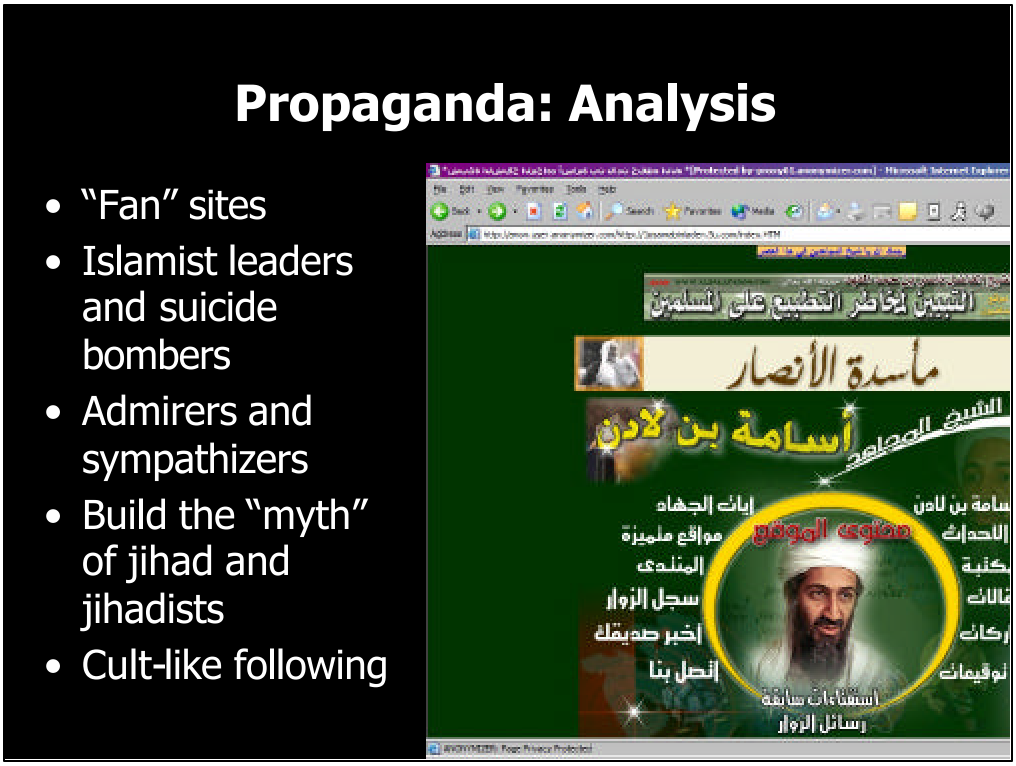
Propaganda: Analysis

- 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
- Many are in Arabic only

The world wide web is already in heavy use by Islamists and sympathizers. There are hundreds of “jihadi” sites online – some news-oriented, some rhetorical, some theological, some militant. The more formal sites provide news articles regarding the fundamentalists’ version of unfolding events in the Middle East and throughout the world, editorials and commentary from religious leaders, photographs of alleged atrocities, and links to other sympathizer sites. These sites are frequently in Arabic, although there are a number of jihadi sites in English, as well. The Arabic-language sites seldom offer an English translation. The ones that do offer a translation sometimes offer different content in the English-language section. That English content mainly focuses on philosophical and theological discussions or attempts to convert the viewer to Islam, and almost always excludes the most inflammatory and violent rhetoric that is pervasive in the Arabic-language portions.

*** Only ~25% of Muslims speak Arabic. Source: NYT article, 10/29/02, citing a Georgetown professor of religion and international affairs, John Esposito

Slide 13



Propaganda: Analysis

- “Fan” sites
- Islamist leaders and suicide bombers
- Admirers and sympathizers
- Build the “myth” of jihad and jihadists
- Cult-like following

Additional forms of propaganda used to spread both Islamic fundamentalism and the cult of the suicide bombers are the “fan” and martyr sites created by admirers and sympathizers.

These sites are generally home-grown in nature, and look much like what a fan of a celebrity might create in homage to the celebrity in question.

A good example of this type of site is the represented by the screen shot here for Mr. Bin Laden <http://1osamabinladen.5u.com/index.htm>. Fan sites work to Islamists’ advantage, as they help to further spread their message, while simultaneously feeding the growing mythology around the jihadists and “martyrs.” Another example is <http://wps.jeeran.com>, which celebrates Hamas suicide bombers.

Overall the trend by Islamic terrorist groups is the use of information technologies, often invented in the West, to deliver an anti Western messages.

Slide 14

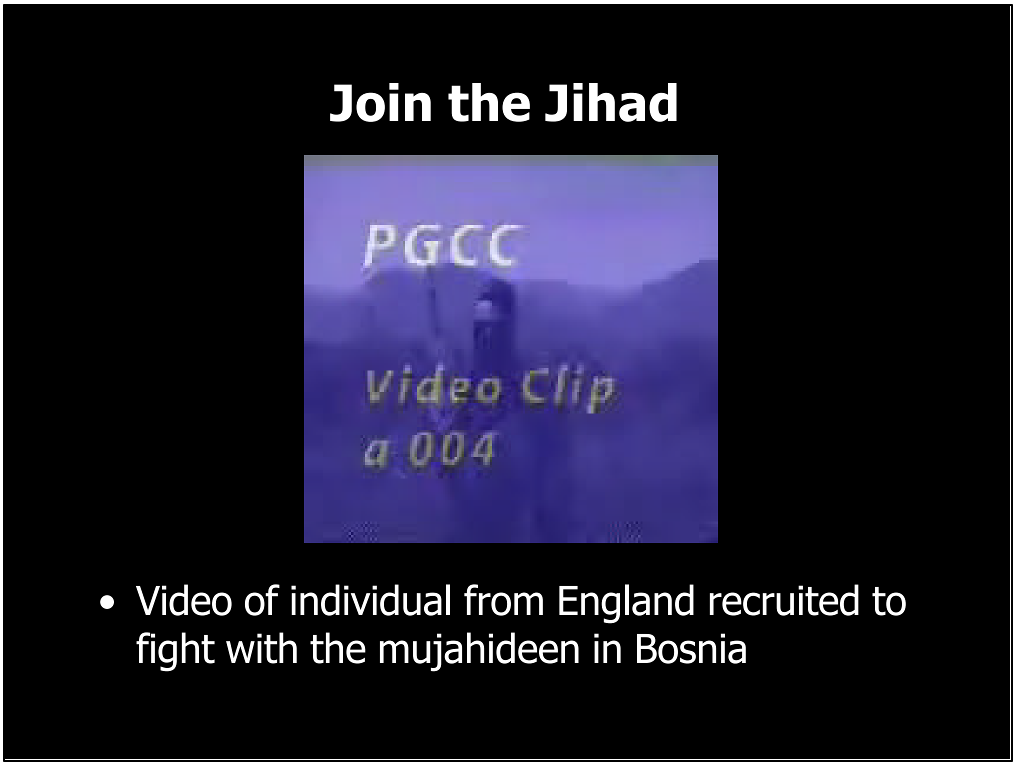
2. Recruitment and Training

Join the Jihad

Once the organization has gotten the attention of potential followers, the next step is to draw them into the hands-on activities of the group.

The next series of slides focuses on online Recruitment and Training.

Slide 15



Join the Jihad

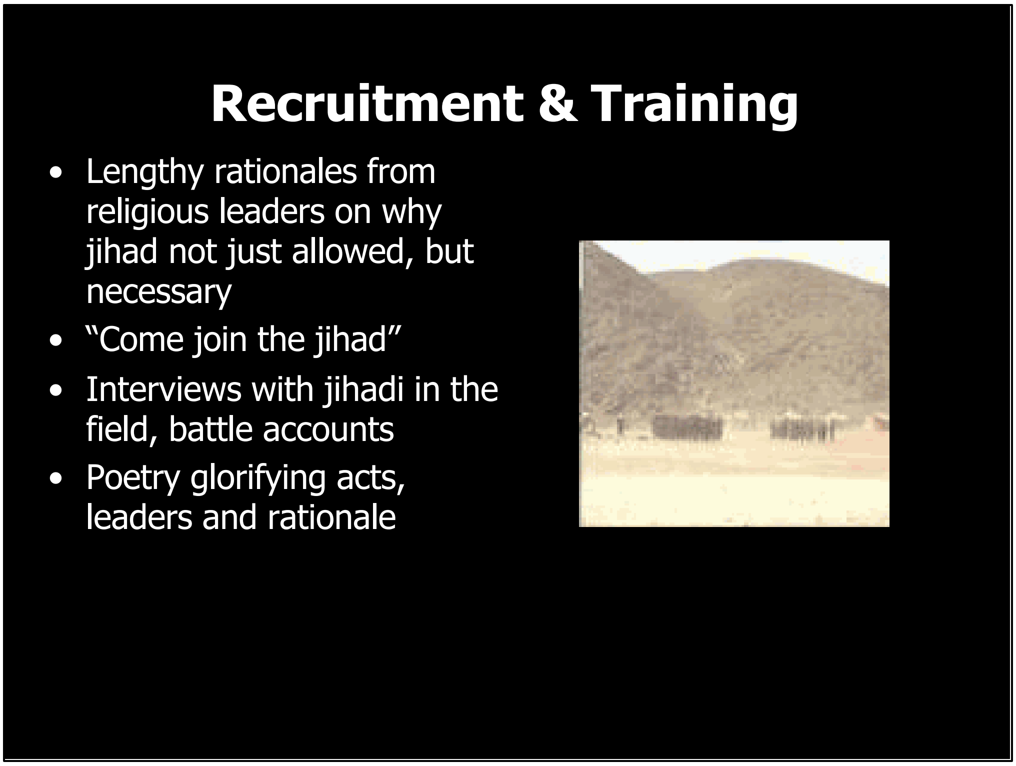
- Video of individual from England recruited to fight with the mujahideen in Bosnia

The video clip on this slide is of an individual from England who says he was recruited to fight with the mujahideen in Bosnia.

He urges “true Muslims” to join the fighting in places such as Bosnia, Chechnya, and Kashmir.

In this video he remarks that at that time (the Bosnian conflict took place between 1992-1995), the mujahideen could readily telephone and fax anywhere in the world from the battlefield, just like any military force.

Slide 16



Recruitment & Training

- Lengthy rationales from religious leaders on why jihad not just allowed, but necessary
- "Come join the jihad"
- Interviews with jihadi in the field, battle accounts
- Poetry glorifying acts, leaders and rationale

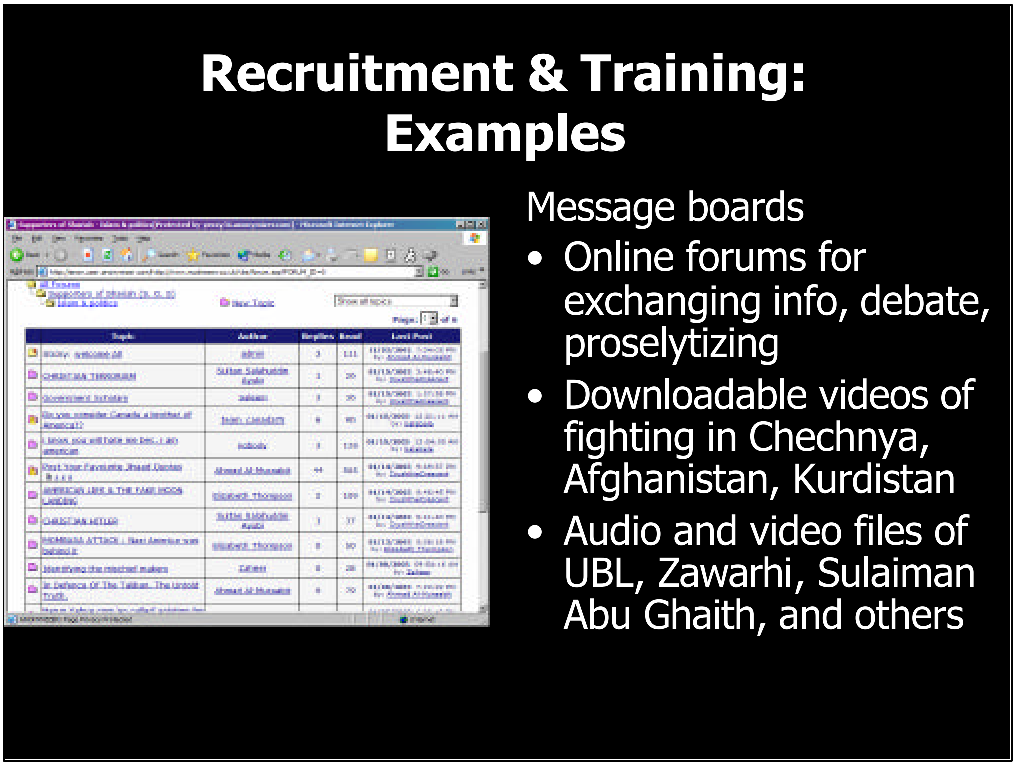
In addition to using the web for propaganda purposes, many of the same websites are used as a recruiting tool for would-be jihadi.

The sites may include bios on famous mujahideen, photos, interviews, and video footage of jihadi training (over-dubbed with inspirational music and messages) conducted at various terrorist training camps.

The footage of the training camps is not dissimilar to U.S. military recruitment ads, with a "Be all that you can be" feel to them, much of it shot in a style reminiscent of western music videos.

The video footage in this slide is also available, along with analysis from <http://www.ciaonet.org/cbr/cbr00/video/cbr_v/cbr_v_1.html>.

Slide 17



Recruitment & Training: Examples

	Topic	Author	Replies	Read	Last Post
	Sticky: welcome all	admin	3	111	[illegible]
	CHRISTIAN TERRORISM	Sultan Salahuddin Ayubi	1	20	[illegible]
	Government Scholars	[illegible]	1	20	[illegible]
	Do you consider Canada a brother of America??	[illegible]	6	[illegible]	[illegible]
	I know you will hate me Dec.. I am american	nobody	3	[illegible]	[illegible]
	Post Your Favourite Jihad Quotes	Ahmad Al-Mussabi	44	[illegible]	[illegible]
	AMERICAN LIES & THE FAKE MOON LANDING	Elizabeth Thompson	2	[illegible]	[illegible]
	CHRISTIAN HITLER	Sultan Salahuddin Ayubi	1	[illegible]	[illegible]
	MOMBASA ATTACK : Nazi America was behind it	Elizabeth Thompson	8	[illegible]	[illegible]
	Identifying the mischief makers	[illegible]	0	[illegible]	[illegible]
	In Defence Of The Taliban. The Untold Truth.	Ahmad Al-Mussabi	0	[illegible]	[illegible]

Message boards

- Online forums for exchanging info, debate, proselytizing
- Downloadable videos of fighting in Chechnya, Afghanistan, Kurdistan
- Audio and video files of UBL, Zawarhi, Sulaiman Abu Ghaith, and others

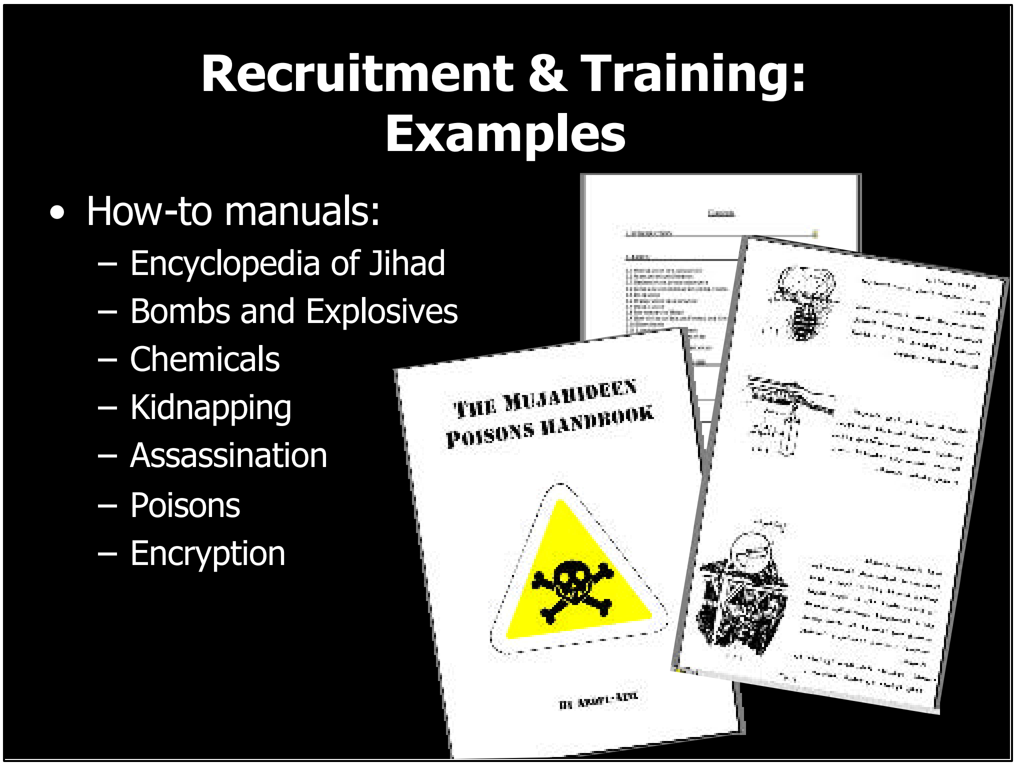
To further engage potential recruits, many sites and message boards provide links to downloadable videos of current and past conflicts.

In the Chechen separatist struggles, for example, the videos are used to provide independent evidence that the mujahideen continue to carry out attacks against the Russian military forces (despite periodic claims to the contrary by state-controlled media) and to serve as a documented history of the jihadi struggle, as well as to emphasize the image of the mujahideen as fierce defenders of the faith.

Message boards are also used to debate jihad, incite and perpetuate anti-American sentiment, and exchange links to other information sources.

The message boards frequently are visited/invaded by decidedly pro-American participants, and profanity-laced, name-calling arguments often break out between the jihadists and those opposed to them. As a result, a number of the more heavily used forums have changed from unmoderated to moderated formats in an effort to keep out pro-American activists or to keep arguments between the two camps from dominating the discussions.

Slide 18



Recruitment & Training: Examples

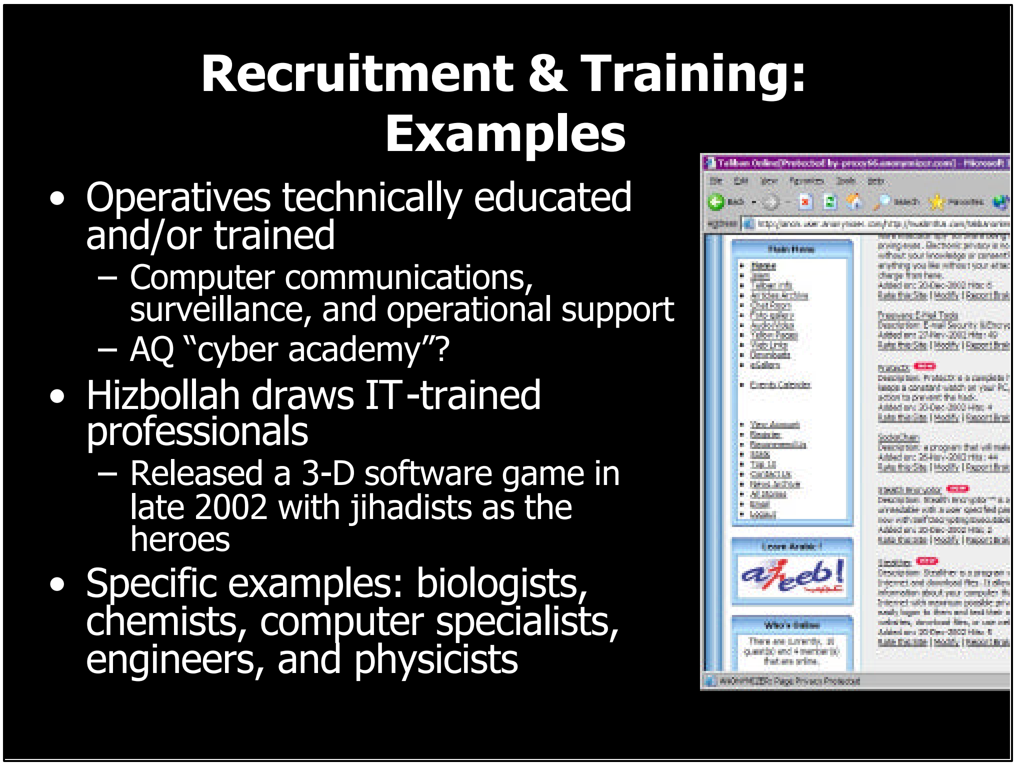
- How-to manuals:
  - Encyclopedia of Jihad
  - Bombs and Explosives
  - Chemicals
  - Kidnapping
  - Assassination
  - Poisons
  - Encryption

Islamic jihad groups also use the Internet to disseminate training materials, either for those who can not attend the training camps, or to get new recruits and sympathizers excited about what they could learn. The manuals, as seen above, are sometimes in Arabic, and sometimes in English.

One of the most infamous of these is the "Encyclopedia of Jihad" [a page of which is on this slide], a 1,000+ page PDF. Many of the sketches in the document appear to have been taken from 1960's-era U.S. military manuals. Most of the text is hand-written in Arabic. This is one of the means used for memorization in the madrassas (religious schools) and in the training camps – transcribing large volumes of information by hand. These manuals are posted in many places on the Internet, amongst the jihadi community. They sometimes borrow liberally from "self-defense" manuals such as "The Poisoner's Handbook" and other volumes favored by Western anti-government advocates.

These manuals include information on encryption and avoiding detection while sending electronic communications.

Slide 19



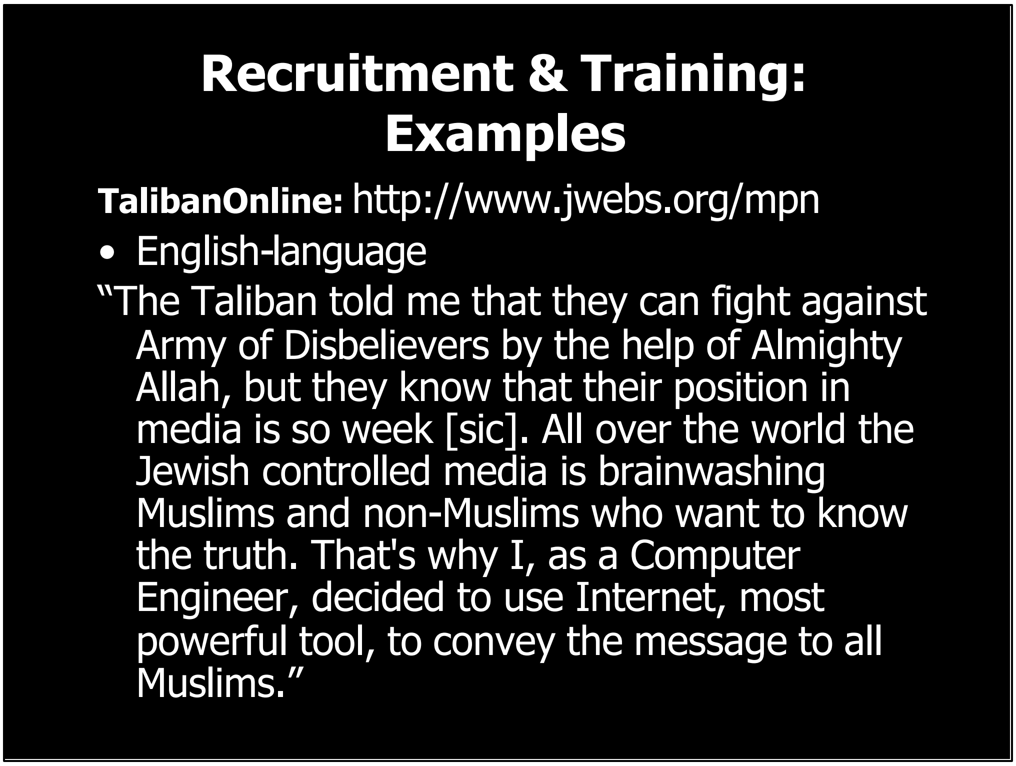
Recruitment & Training: Examples

- Operatives technically educated and/or trained
  - Computer communications, surveillance, and operational support
  - AQ “cyber academy”?
- Hizbollah draws IT-trained professionals
  - Released a 3-D software game in late 2002 with jihadists as the heroes
- Specific examples: biologists, chemists, computer specialists, engineers, and physicists

Individuals throughout the Islamic jihad, especially at the highest operational levels, show knowledge that indicates a strong technological proficiency. Many of these individuals have technical degrees or training, and use of computer technology is routine. For example, a 1999 report by the Library of Congress’ Federal Research Division states, “Osama bin Laden also recruits highly skilled professionals in the fields of engineering, medicine, chemistry, physics, **computer programming, communications**, and so forth. […] the terrorists of the 1990s who have carried out major operations have included biologists, chemists, computer specialists, engineers, and physicists.” [1] A number of reports indicate that recruits proceed to specialized training camps and after an initial assessment, receive specific training in the use of computers for communications, surveillance, and operational support at a minimum. At least some reports have suggested that, at least for a time, a safe house in Pakistan was an AQ “cyber academy”, used to train select recruits to conduct overt and covert cyber attacks for multiple purposes.

[1] <http://www.fas.org/irp/threat/frd.html>

Slide 20



Recruitment & Training: Examples

TalibanOnline: http://www.jwebs.org/mpn

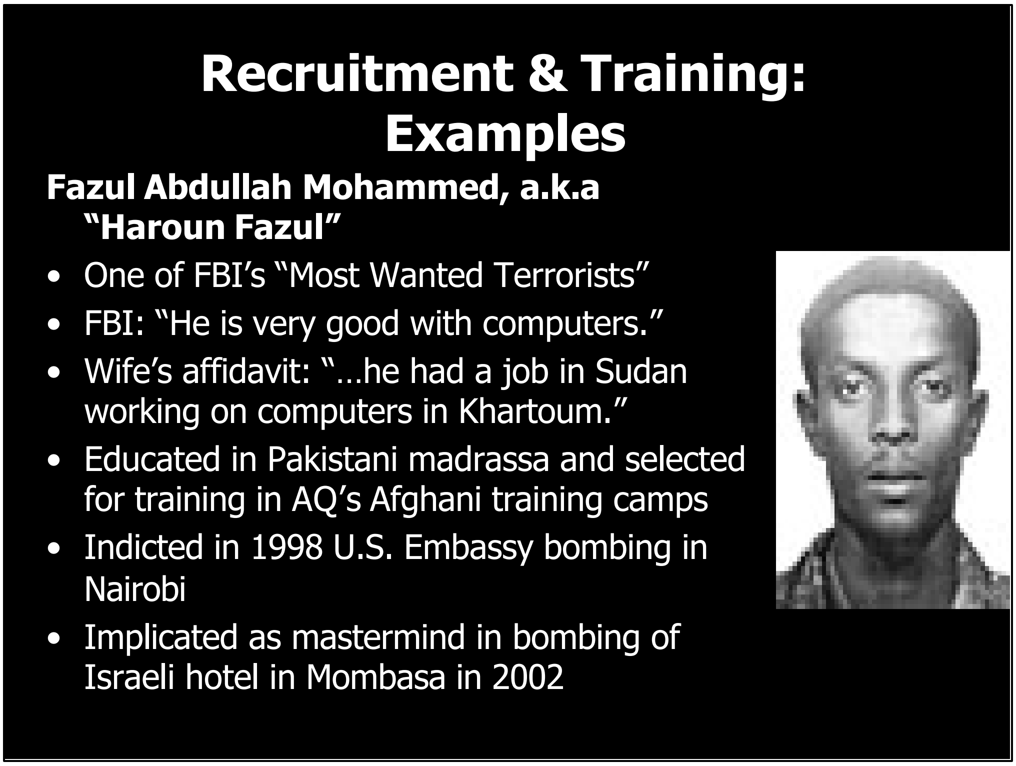
- English-language

"The Taliban told me that they can fight against Army of Disbelievers by the help of Almighty Allah, but they know that their position in media is so week [sic]. All over the world the Jewish controlled media is brainwashing Muslims and non-Muslims who want to know the truth. That's why I, as a Computer Engineer, decided to use Internet, most powerful tool, to convey the message to all Muslims."

One of the sites purporting to be a conduit for the Taliban is "TalibanOnline", run by an individual who says that he became a fundamentalist Muslim and Taliban supporter in October 2001. His conversion came after visiting an Afghan refugee camp in Peshawar, and he decided to create this particular (there are several) Taliban Online site because "The Taliban told me that they can fight against Army of Disbelievers by the help of Almighty Allah, but they know that their position in media is so week [sic]. All over the world the Jewish controlled media is brainwashing Muslims and non-Muslims who want to know the truth. That's why I, as a Computer Engineer, decided to use Internet, most powerful tool, to convey the message to all Muslims." [1]

[1] <http://www.ciaonet.org/cbr/cbr00/video/cbr_v/cbr_v_1.html>

Slide 21



Recruitment & Training: Examples

Fazul Abdullah Mohammed, a.k.a "Haroun Fazul"

- One of FBI's "Most Wanted Terrorists"
- FBI: "He is very good with computers."
- Wife's affidavit: "…he had a job in Sudan working on computers in Khartoum."
- Educated in Pakistani madrassa and selected for training in AQ's Afghani training camps
- Indicted in 1998 U.S. Embassy bombing in Nairobi
- Implicated as mastermind in bombing of Israeli hotel in Mombasa in 2002

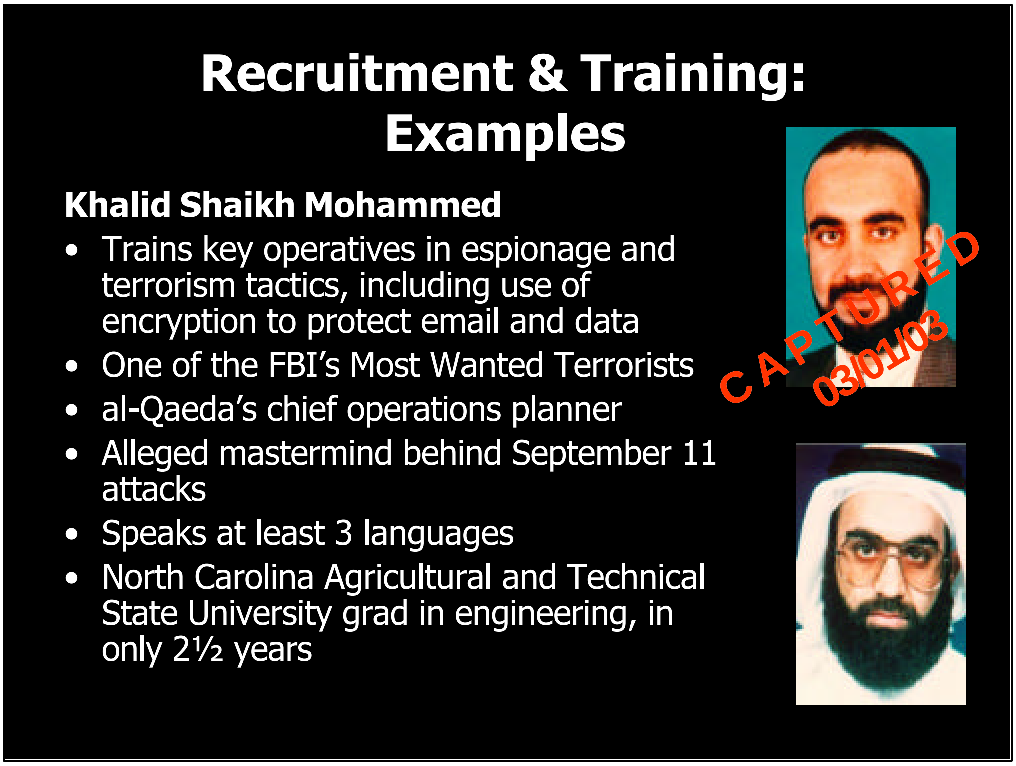
PBS's "Frontline" program did an up-close look at another of the FBI's "Most Wanted Terrorists", Fazul Abdullah Mohammed. The FBI describes Fazul as "very good with computers". [1] Fazul comes from the Comoros Islands off the coast of Africa, where he was educated in a madrassa (an Islamic religious school). He was selected to receive further education at a Pakistani madrassa, and ultimately Fazul was sent to an AQ terrorist training camp and then back to Africa to conduct covert operations. His cover was first as a computer student, then as a computer worker, according to a deposition given by his wife during the investigation into the 1998 U.S. Embassy bombing in Nairobi [2]. More recently, Fazul is said to have masterminded the attack in Mombasa on an Israeli hotel [3].

[1] <http://www.fbi.gov/mostwant/terrorists/termohammed.htm>

[2] <http://www.pbs.org/wgbh/pages/frontline/shows/saudi/fazul> - includes transcript of wife's deposition in relation to the Nairobi U.S. Embassy bombing in 1998.

[3]<http://www.haaretzdaily.com/hasen/pages/ShArt.jhtml?itemNo=237403&contrassID=2&subContrassID=1&sbSubContrassID=0> and <http://www.cnn.com/2002/WORLD/africa/12/02/kenya.probe/index.html>

Slide 22



Recruitment & Training: Examples

Khalid Shaikh Mohammed

- Trains key operatives in espionage and terrorism tactics, including use of encryption to protect email and data
- One of the FBI's Most Wanted Terrorists
- al-Qaeda's chief operations planner
- Alleged mastermind behind September 11 attacks
- Speaks at least 3 languages
- North Carolina Agricultural and Technical State University grad in engineering, in only 2½ years

CAPTURED
03/01/03

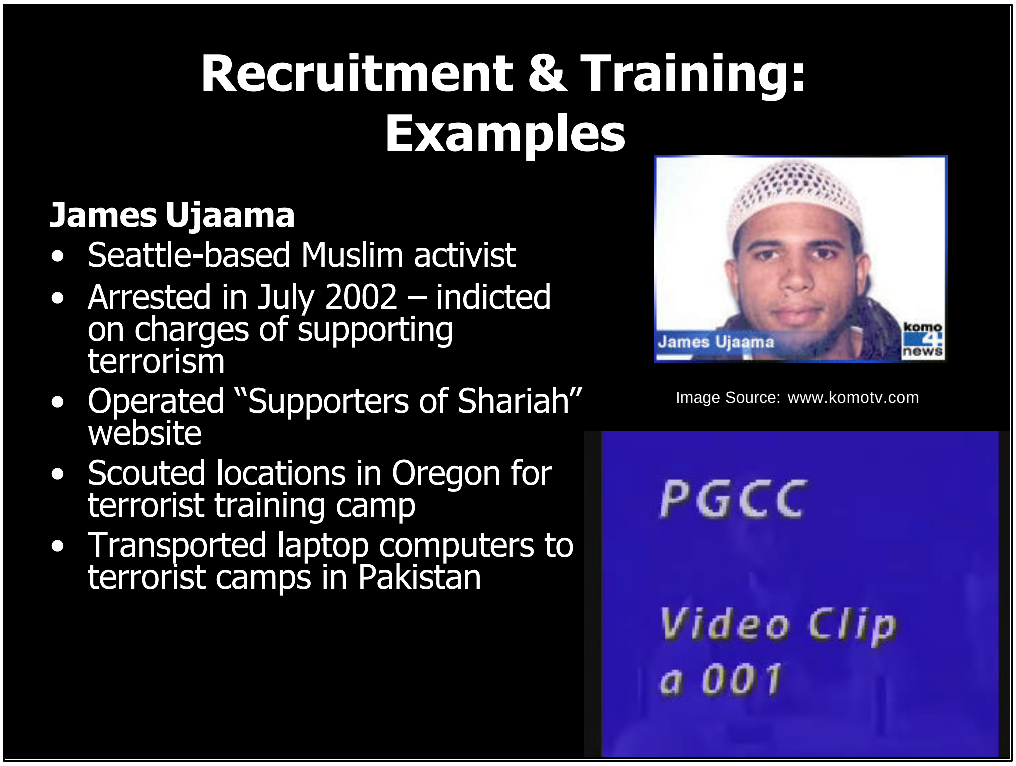
Khalid Shaikh Mohammed, captured on March 1, 2003, was one of the FBI's "Most Wanted Terrorists". [1] The U.S. intelligence community believes that Khalid became AQ's top operations strategist prior to his capture. He was indicted for having masterminded a plot to bomb U.S. airliners flying southeast Asian routes, and he is probably the mastermind behind the September 11 attacks. Some news accounts [2] say that one of the Pakistanis involved with the kidnapping and murder of WSJ reporter Daniel Pearl claims that it was Khalid who actually cut Pearl's throat, on video. He is also reportedly Ramzi Yousef's uncle. Khalid is multi-lingual and well-educated, including a degree in engineering from North Carolina Agricultural and Technical School (which he completed in only 2½ yrs.). He is said to have trained Mohammed Mansour Jabarah (Canadian citizen of Kuwaiti heritage recruited as AQ lead in multiple disrupted Indonesian operations) and other high-level AQ operatives in use of encryption, among other espionage skills.

[1] <http://www.fbi.gov/mostwant/terrorists/terkmohammed.htm>

[2] <http://www.time.com/time/asia/covers/1030127/ksm.html>, <http://www.hinduonnet.com/thehindu/2002/09/16/stories/2002091604181200.htm> and <http://www.smh.com.au/articles/2003/03/04/1046540197365.html>

Also, generally <http://asia.cnn.com/2002/WORLD/asiapcf/southeast/10/29/asia.jihad.2>

Slide 23



Recruitment & Training: Examples

James Ujaama

- Seattle-based Muslim activist
- Arrested in July 2002 – indicted on charges of supporting terrorism
- Operated "Supporters of Shariah" website
- Scouted locations in Oregon for terrorist training camp
- Transported laptop computers to terrorist camps in Pakistan

James Ujaama
komo 4 news

Image Source: www.komotv.com

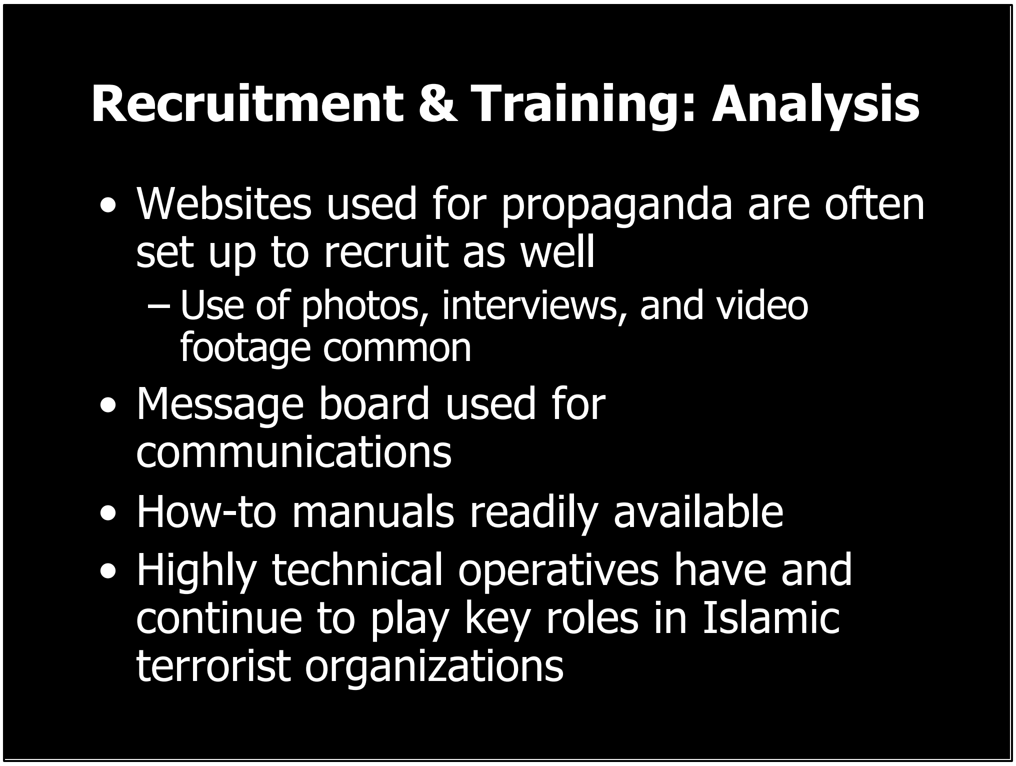
PGCC
Video Clip
a 001

In the case of alleged al-Qaeda member James Ujaama [1], Seattle WA-based Muslim activist and **computer engineer**, an un-indicted co-conspirator is alleged to have made use of Ujaama's services to build and maintain the www.supportersofshariah.com website. This website is run under the direction of Sheik Abu Hamza al-Masri, who is the head of the notorious Finsbury Park mosque in London, England. The website is used to promote a conservative Islamic agenda, encourage jihad, publish al-Masri's sermons and lectures, and recruit new members. In Ujaama's case, it appears that he may have been brought into the organization to make use of his computer skills.

The indictment against Ujaama, filed in August 2002, accuses him of not only designing and administering the website, but also of providing computer support services to al-Qaeda (including taking laptops to Afghanistan training camps) and also of scouting locations in the U.S., possibly to locate a terrorist training facility.

[1] <http://news.findlaw.com/hdocs/docs/terrorism/usujaama82802ind.pdf>

Slide 24



Recruitment & Training: Analysis

- Websites used for propaganda are often set up to recruit as well
  - Use of photos, interviews, and video footage common
- Message board used for communications
- How-to manuals readily available
- Highly technical operatives have and continue to play key roles in Islamic terrorist organizations

Websites used for propaganda are often set up to recruit as well.

The sites may include bios on famous mujahideen or videos of jihadi training (over-dubbed with inspirational music and messages) conducted at various terrorist training camps.

Message board used for recruitment and communications.

How-to manuals are readily available to any who wish to learn. These manuals have included information on encryption and avoiding detection while sending electronic communications.

As the examples in this section show, highly technical operatives have and continue to play key roles in Islamic Terrorist organizations. As we have seen in the propaganda section of this report the trend is the use of information technologies to recruit and propagate training materials.

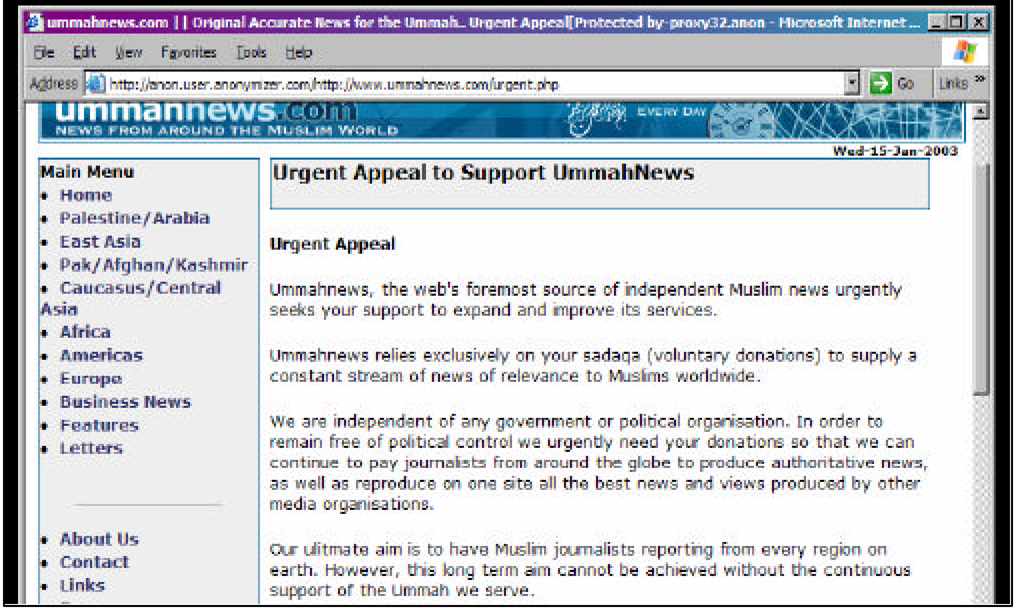
Slide 25

3: Fundraising

How Technology Helps
Terrorists Fundraise

Slide 26

How To Pay For It All



ummahnews.com | | Original Accurate News for the Ummah.. Urgent Appeal[Protected by-proxy32.anon - Microsoft Internet ...

http://anon.user.anonymizer.com/http://www.ummahnews.com/urgent.php

Wed-15-Jan-2003

Urgent Appeal to Support UmmahNews

Urgent Appeal

Ummahnews, the web's foremost source of independent Muslim news urgently seeks your support to expand and improve its services.

Ummahnews relies exclusively on your sadaqa (voluntary donations) to supply a constant stream of news of relevance to Muslims worldwide.

We are independent of any government or political organisation. In order to remain free of political control we urgently need your donations so that we can continue to pay journalists from around the globe to produce authoritative news, as well as reproduce on one site all the best news and views produced by other media organisations.

Our ultimate aim is to have Muslim journalists reporting from every region on earth. However, this long term aim cannot be achieved without the continuous support of the Ummah we serve.

Islamic terrorists are using cyberspace and cyber technology to raise money in a number of ways.

A common approach for terrorist organizations is to channel funds from legitimate charities, but there is evidence that they are raising funds through other means as well, including criminal activities.

For example, on the Council on Foreign Relations' "Terrorism: Questions and Answers" website, the question "How is al-Qaeda funded?" is answered (in part): "… [UBL] established companies to provide income and charities that act as fronts. In addition protection schemes, **credit-card fraud**, and drug smuggling are other possible sources of money." [1] Legitimate businesses, charities, credit-card fraud, and drug smuggling today all rely heavily on computer technology to operate, and any organization active in any of these activities must be computer-savvy.

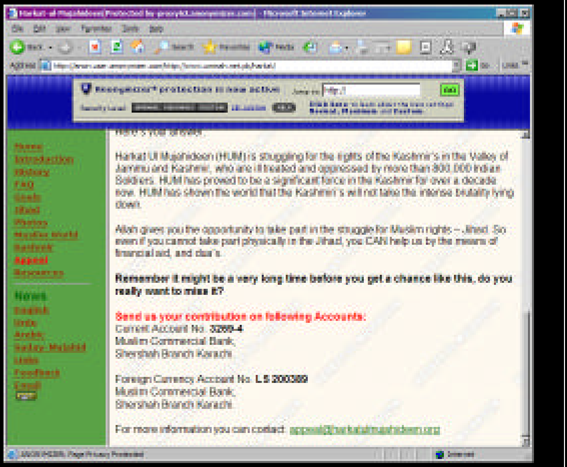
This slide illustrates an appeal for funds to support an Islamic news organization.

[1] <http://www.terrorismanswers.com/groups/alqaeda3.html>

Slide 27

Fundraising: Examples

- News websites solicit funds to support their efforts
  - Often include mailing addresses or wire transfer accounts for contributions
- Advertising dollars from Muslim businesses



Harkat-ul-Mujahideen| Protected by proxy4.anonymizer.com| - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Anonymizer® protection is now active
Jump to: http://
Go
Security Level
Home
Introduction
History
FAQ
Goals
Jihad
Photos
Muslim World
Kashmir
Appeal
Resources
News
English
Urdu
Arabic
Sadaye Mujahid
Links
Feedback
Email
Internet

Here's your answer:

Harkat Ul Mujahideen (HUM) is struggling for the rights of the Kashmir's in the Valley of Jammu and Kashmir, who are ill treated and oppressed by more than 800,000 Indian Soldiers. HUM has proved to be a significant force in the Kashmir for over a decade now. HUM has shown the world that the Kashmir's will not take the intense brutality lying down.

Allah gives you the opportunity to take part in the struggle for Muslim rights – Jihad. So even if you cannot take part physically in the Jihad, you CAN help us by the means of financial aid, and dua's.

Remember it might be a very long time before you get a chance like this, do you really want to miss it?

Send us your contribution on following Accounts:
Current Account No. **3289-4**
Muslim Commercial Bank,
Shershah Branch Karachi

Foreign Currency Account No. **LS 200389**
Muslim Commercial Bank,
Shershah Branch Karachi

For more information you can contact: appeal@harkatulmujahideen.org

Islamic news viewers are often asked to send contributions to support the mujahideen and/or the "victims of oppression".

These requests generally include, at minimum, a mailing address and an email account.

Often these solicitations including wire transfer account information, including instructions on how to do the wire transfer.

The news sites may also solicit advertising from faithful Muslim businesses.

Slide 28

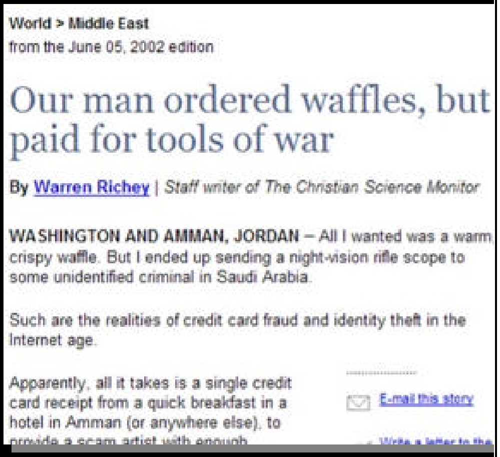
Fundraising: Examples

1998: Lebanese group

- Ties to Middle Eastern terrorist groups and counterfeit credit cards

2001 Journalists for Christian Science Monitor

- Credit card info stolen at hotel restaurant in Jordan
- Purchases of military equipment in reporter's name shipped to Saudi Arabia



World > Middle East
from the June 05, 2002 edition

Our man ordered waffles, but paid for tools of war

By Warren Richey | *Staff writer of The Christian Science Monitor*

WASHINGTON AND AMMAN, JORDAN – All I wanted was a warm, crispy waffle. But I ended up sending a night-vision rifle scope to some unidentified criminal in Saudi Arabia.

Such are the realities of credit card fraud and identity theft in the Internet age.

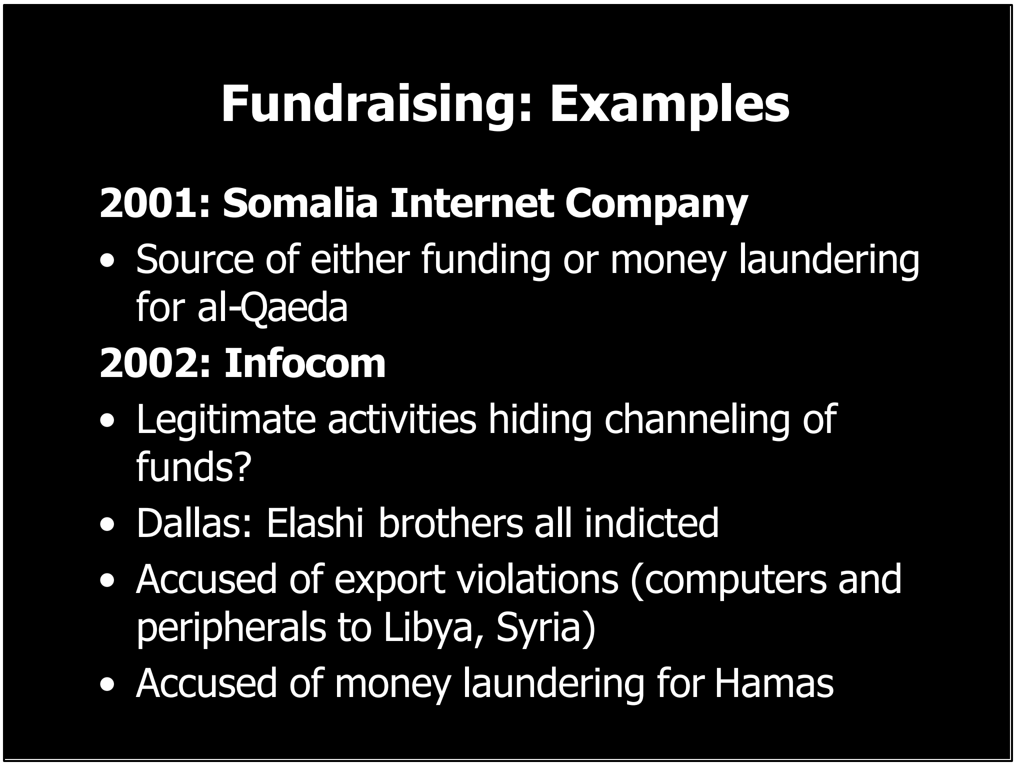
Apparently, all it takes is a single credit card receipt from a quick breakfast in a hotel in Amman (or anywhere else), to provide a scam artist with enough

Islamic terrorist groups have been using credit card fraud since the late 1990's to finance their activities. Richard A. Rohde, Deputy Assistant Director - Office of Investigations, U.S. Secret Service, before the Subcommittee On Technology, Terrorism And Government Information Of The Senate Committee On The Judiciary, on February 24, 1998 that an organized group of Lebanese nationals are responsible for counterfeiting credit cards that were found with Middle Eastern terrorist group members.[1]

A journalist for the Christian Science Monitor recounted last year (2002) an incident of how he was the victim of credit card fraud during a trip to Amman, Jordan in late 2001.[2] Although he never lost his card or any receipts during his trip, "Transaction records reveal that the first attempted fraudulent purchase was made on the same day that I returned to the U.S. The $3,100 transaction for two Russian-made night-vision rifle scopes and a more high-tech miniature night-vision scope was refused because it exceeded the single-purchase limit on my card. Roughly a month later, however, someone submitted a scaled-down version of the same order and it was accepted. According to my credit card company's fraud investigators, the order included one Russian night-vision rifle scope, and a US-built range finder, an instrument that calculates the distance to a potential target." The purchases and shipping were made in the reporter's name, and the items were shipped to an address in Riyadh. Shortly after the journalist discovered the fraud, he found that a colleague at the same paper had the same thing happen to her, a few weeks later. The point in common? The restaurant of the hotel where both stayed in Amman. Although the incident cannot conclusively be specifically tied to Islamic terrorists per se, it is just one example of the level of activity and trafficking in stolen credit cards in the Middle East (jihadists' recruitment base), tied to logistics and the purchase of military-style equipment.

[1] <http://www.fas.org/irp/congress/1998_hr/s980224r.htm>

[2] <http://www.csmonitor.com/2002/0605/p01s04-wome.html>



Fundraising: Examples

2001: Somalia Internet Company

- Source of either funding or money laundering for al-Qaeda

2002: Infocom

- Legitimate activities hiding channeling of funds?
- Dallas: Elashi brothers all indicted
- Accused of export violations (computers and peripherals to Libya, Syria)
- Accused of money laundering for Hamas

The Somalia Internet Company, Somalia's only ISP, was effectively shut down in 2001 after its assets were frozen under U.S. and U.N. Security Council sanctions.[1] The sanctions were ordered on the belief that the company is a source of either funding or money laundering for al-Qaeda. The company denies links to terrorism, but as of February 2003, they remain under sanctions.

Infocom – in 2002, a Federal indictment was issued against a suburban Dallas-based computer company called Infocom. The indictment was against the company and four brothers who were executives and professional staff there, including the CEO. [2] A fifth brother, plus an acknowledged Hamas leader and his wife – who is cousin to the brothers – were also named. The brothers are accused in the indictment [3] of using Infocom to export computer equipment and programs to countries banned from possessing them (specifically, Libya and Syria) and of using Infocom to launder money for Hamas, by accepting "investments" in Infocom in their cousin's name that really came from her husband, a high-ranking Hamas member. Payments were then made back from Infocom to the cousin.

[1] <http://news.bbc.co.uk/1/hi/world/africa/1672220.stm>

[2] <http://www.cnn.com/2002/US/Southwest/12/18/hamas.arrests/>

[3] <http://news.findlaw.com/wsj/docs/infocom/uselashi121702sind.pdf>

Slide 30

Fundraising: Examples

al-Qaeda terrorist cell in Spain

- Used stolen credit cards in fictitious sales scams and for numerous other purchases
- Kept purchases under amounts requiring identification
- Stole telephone and credit cards for communications
- Opened bank accounts - money was sent to and from countries such as Pakistan and Afghanistan

According to testimony by Dennis Lormel (Chief, Terrorist Financial Review Group, FBI) before the Senate Judiciary Subcommittee on Technology, Terrorism and Government Information (July 9, 2002), "… an Al-Qaeda terrorist cell in Spain used stolen credit cards in fictitious sales scams and for numerous other purchases for the cell.

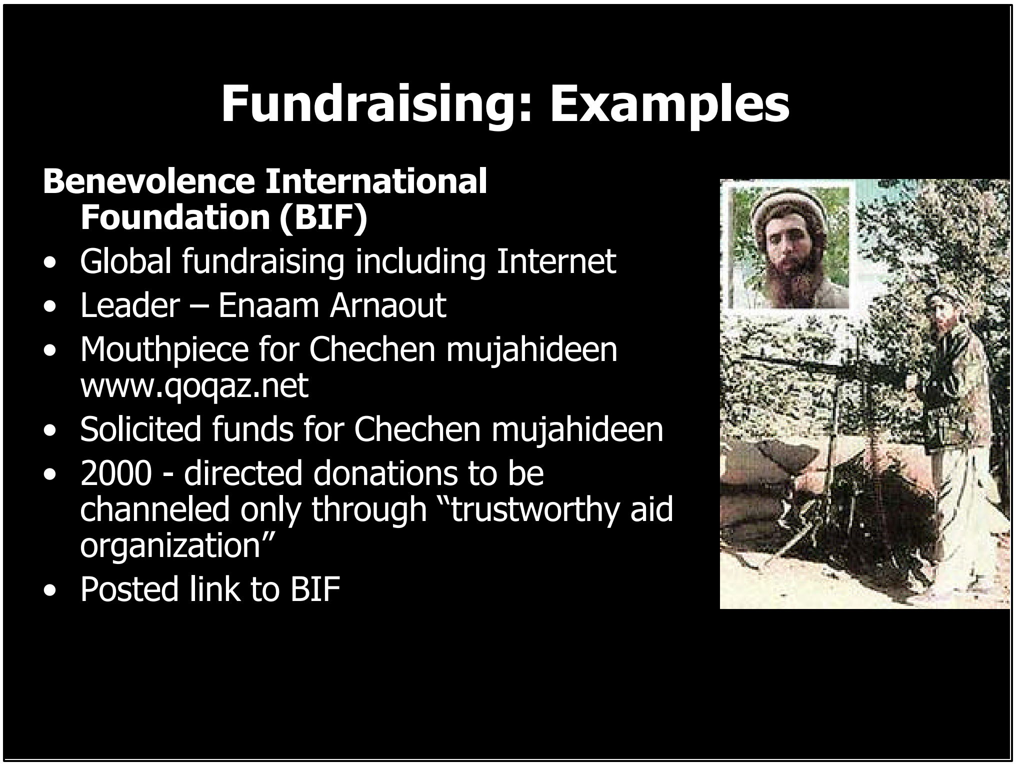
They kept purchases below amounts where identification would be presented.

They also used stolen telephone and credit cards for communications back to Pakistan, Afghanistan, Lebanon, etc.

Extensive use of false passports and travel documents were used to open bank accounts where money for the mujahadin movement was sent to and from countries such as Pakistan, Afghanistan, etc." [1]

[1] <http://www.fbi.gov/congress/congress02/idtheft.htm>

Slide 31



Fundraising: Examples

Benevolence International Foundation (BIF)

- Global fundraising including Internet
- Leader – Enaam Arnaout
- Mouthpiece for Chechen mujahideen www.qoqaz.net
- Solicited funds for Chechen mujahideen
- 2000 - directed donations to be channeled only through "trustworthy aid organization"
- Posted link to BIF

After September 11, 2001, one of the most important actions undertaken internationally was the introduction of sanctions against large numbers of businesses and charities that the Allies have linked to terrorism. [1] The sanctions have been initiated under the premise that choking off funding sources of terrorism is potentially one of the most effective ways to limit terrorist activities. Among the list of hundreds of entities, Benevolence International Foundation stands out. Based in Chicago, Benevolence International Foundation (BIF) was run by Enaam Arnaout [2]. qoqaz.net, the Chechen jihadi site with ongoing links to the global Islamic jihad, was used to solicit funds to support the mujahideen in Chechnya, funneling the funds through BIF in 2000. The leader of the Chechen mujahideen at that time was Ibn al Khattab (deceased, early 2002).

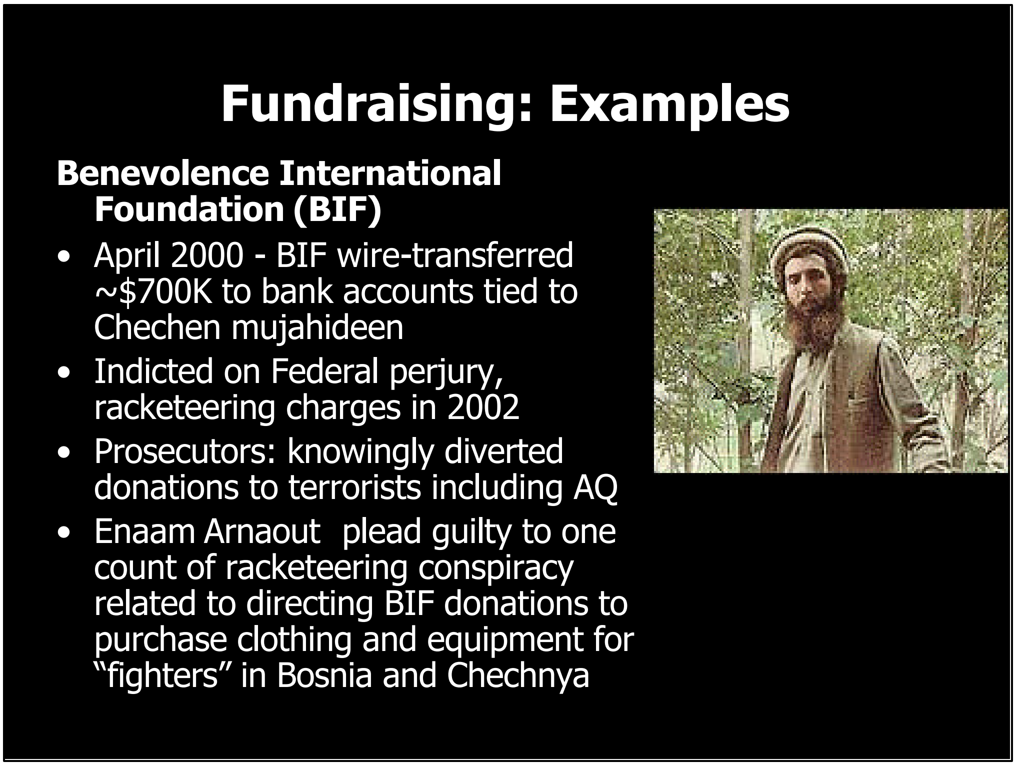
Khattab, through the Qoqaz website, told supporters to wait until a "trustworthy aid organization" to work with them could be identified. The Qoqaz site has posted that "There is one trusted agency that has set up operations in the region and we will be posting their contact and bank details, etc. on the Internet very soon insha-Allah. This is the only aid agency that the Qoqaz web-sites trust and recommend the people to give their donations to."

Shortly after this posting, the Qoqaz site created active donations links to two charities. One was BIF.

[1] <http://www.ustreas.gov/offices/enforcement/ofac/sanctions/terrorism.html>

[2] AP photo, located at <http://www.cbsnews.com/stories/2002/04/30/attack/main507629.shtml>

Slide 32



Fundraising: Examples

Benevolence International Foundation (BIF)

- April 2000 - BIF wire-transferred ~$700K to bank accounts tied to Chechen mujahideen
- Indicted on Federal perjury, racketeering charges in 2002
- Prosecutors: knowingly diverted donations to terrorists including AQ
- Enaam Arnaout plead guilty to one count of racketeering conspiracy related to directing BIF donations to purchase clothing and equipment for "fighters" in Bosnia and Chechnya

Between January and April of 2000, BIF wire transferred nearly $700,000 to Chechen separatist-linked bank accounts in Georgia (FSU), Azerbaijan, Russia, and Latvia.

Arnaout was indicted, along with BIF, in 2002 on a number of charges, including perjury and racketeering.[1]

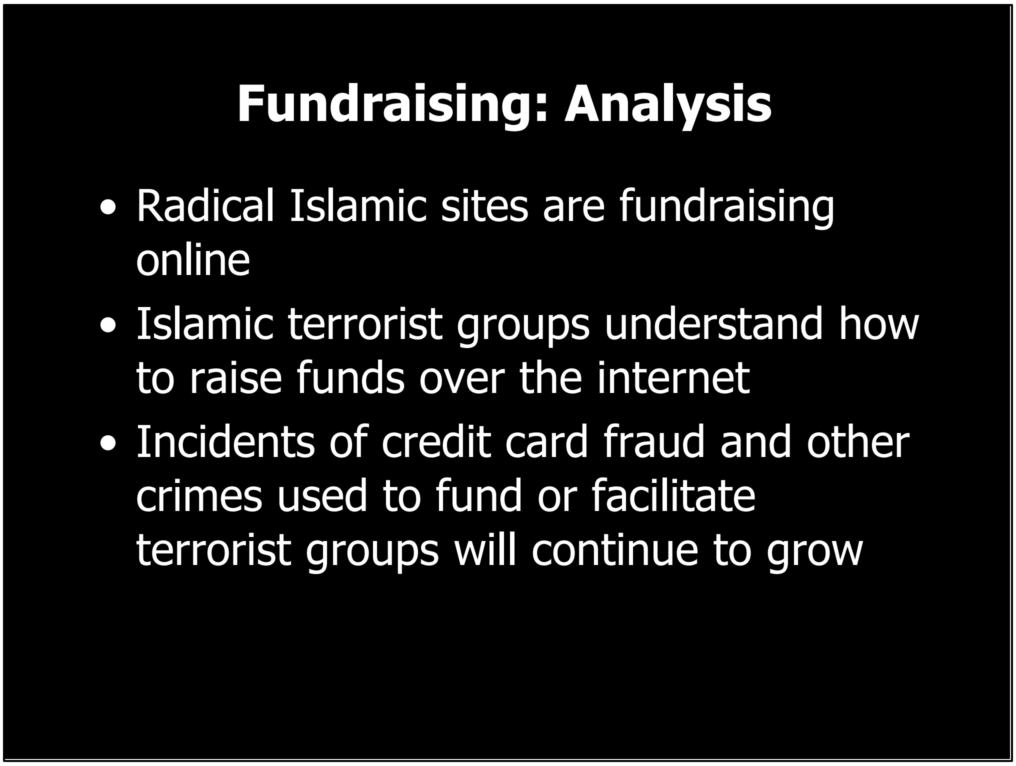
Prosecutors said they had proof, in the form of correspondence and photos, of ties between Arnaout and Usama bin Laden.

In February 2003, Arnaout reached a plea agreement with prosecutors [2]. Arnaout plead guilty to one count of racketeering conspiracy, related to directing BIF donations to purchase clothing and equipment for "fighters" in Bosnia and Chechnya, without disclosing this use of funds to donors.

[1] <http://news.findlaw.com/hdocs/docs/terrorism/usbif42902cmp.pdf>

[2] <http://www.washingtonpost.com/wp-dyn/articles/A51490-2003Feb10.html>

Slide 33



Fundraising: Analysis

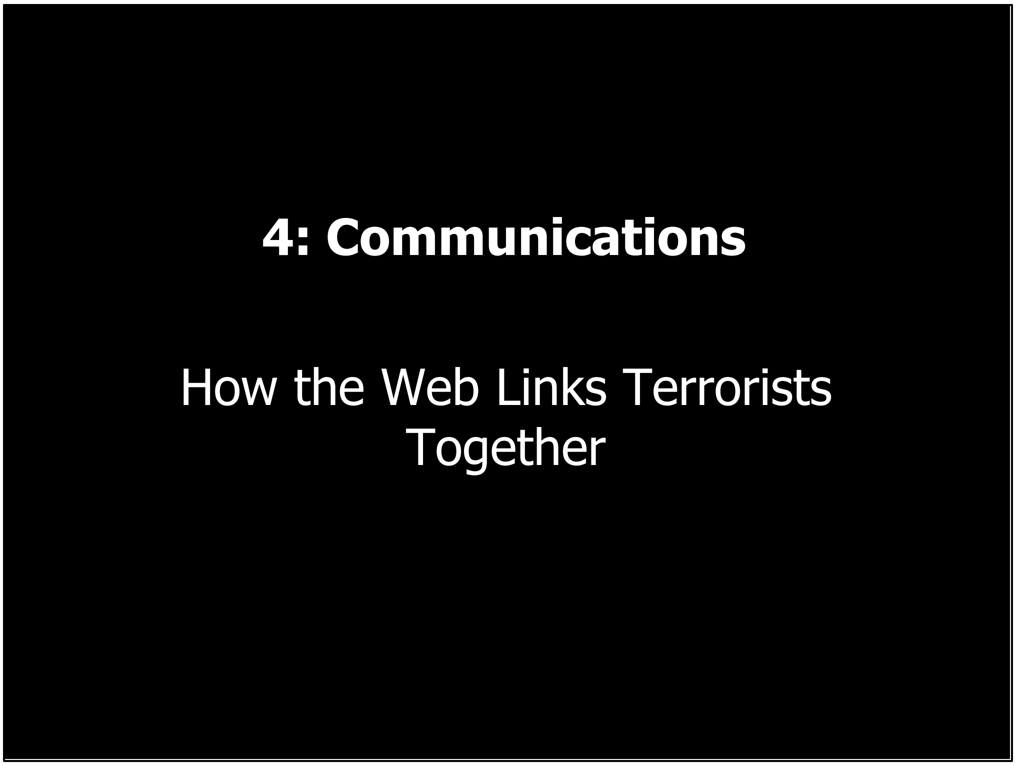
- Radical Islamic sites are fundraising online
- Islamic terrorist groups understand how to raise funds over the internet
- Incidents of credit card fraud and other crimes used to fund or facilitate terrorist groups will continue to grow

As shown in the previous examples radical Islamic web sites and the individuals and organizations that run them are fundraising online.

Islamic terrorist groups understand how to raise funds over the internet.

Clearly information technologies facilitating the easy transfer of funds are of benefit to Islamic terrorist groups.

With no easy solution to the policing of these activities incidents of credit card fraud and other crimes used to fund or facilitate terrorist groups will continue to grow.



4: Communications

How the Web Links Terrorists Together

Slide 35

Keeping in Touch

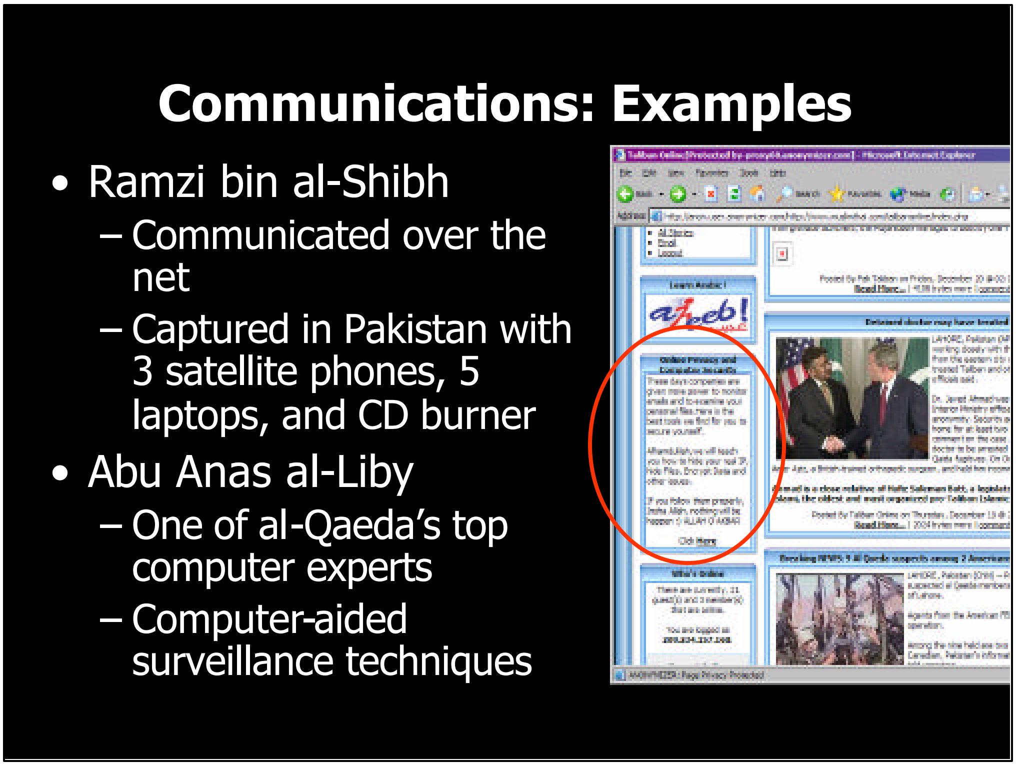
While many in the military, law enforcement, and intelligence communities disagree about the ability and likelihood of Islamist terrorists conducting cyber attacks on the West, there is no doubt that terrorists are harnessing the Internet and computer technology in general as communications tools.

Numerous indictments in terrorism cases cite the use of emails, sometimes coded or encrypted, by alleged operatives and associates to communicate across the globe [1].

Certainly it is well-established that Islamic terrorists use computers as a part of their normal routines, since media accounts abound of the seizure of laptop and desktop computers containing evidence of alleged terrorist activities in locations around the world where terrorist suspects have been arrested or sought.

[1] Examples: United States. v. Ramzi Yusef; Atta et al; United States v. Zacarias Moussaoui aka Shaqil, aka Abu Khalid al Sahraw …

Slide 36



Communications: Examples

- Ramzi bin al-Shibh
  - Communicated over the net
  - Captured in Pakistan with 3 satellite phones, 5 laptops, and CD burner
- Abu Anas al-Liby
  - One of al-Qaeda's top computer experts
  - Computer-aided surveillance techniques

Ramzi bin al-Shibh was captured on September 11, 2002. He is an AQ member who was indicted, along with others, as a co-conspirator with Zacharias Moussaoui in plotting and carrying out the September 11, 2001 attacks on NYC and Washington, D.C. [1] It is believed that bin al-Shibh was originally supposed to be among the hijackers, but he was unable to gain entry to the U.S. When he was captured, the location of the apartment where he and four other AQ members were hiding was traced by U.S. FBI agents by tracking to that building a satellite phone call made by someone in the group [2]. Bin al-Shibh was captured after a reported three-hour gun battle with Pakistani police and intelligence officers. In the apartment were, reportedly, three satellite phones, five laptops, and a CD burner, along with over 500 CDs.[3] He had apparently been living there for months, communicating w/other AQ members on the Internet via a satellite phone linkup.[4]

One of the FBI's "Most Wanted Terrorists", Abu Anas al-Liby, is said to be one of al-Qaeda's top computer experts and that he trains others in the organization on how to use computers. According to testimony from the Nairobi embassy bombing trial, al-Liby worked closely with Usama bin Laden (and was indicted along with him by a Federal Grand Jury) during the years bin Laden based his operations in the Sudan, and provided training to would-be al-Qaeda members on the use of computers in relation to their work:

Q. You mentioned a person by the name of Abu Anas al Liby. Did he ever have any special expertise?

A. Could you repeat the question?

Q. Abu Anas al Liby, did you have any specialty within al Qaeda?

A. Yes.

Q. What was that?

A. He's -- he run our computers. He's a computer engineer."[5]

The witness went on to say that al-Liby provided training to individuals on computer-aided surveillance techniques.

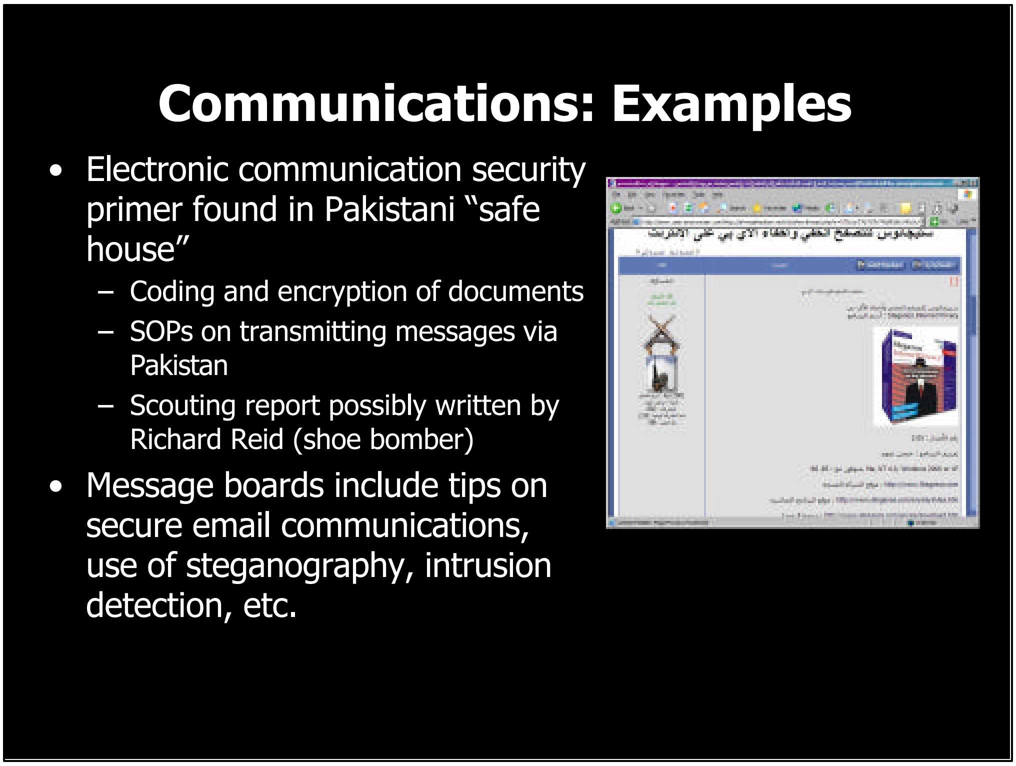
The red circle on this slide highlights an example of an Islamic web site providing a link to a service that teaches users how to communicate securely over the Internet.

[1] <http://www.fbi.gov/pressrel/speeches/mous.pdf>

[2] <http://www.ict.org.il/spotlight/det.cfm?id=825>

[3] & [4] <http://www.nytimes.com/2002/11/01/international/asia/01STAN.html>

[5] <http://news.findlaw.com/hdocs/docs/binladen/binladen20601tt.pdf>, p.333, witness, Jamal Al-Fadhl



Communications: Examples

- Electronic communication security primer found in Pakistani "safe house"
  - Coding and encryption of documents
  - SOPs on transmitting messages via Pakistan
  - Scouting report possibly written by Richard Reid (shoe bomber)
- Message boards include tips on secure email communications, use of steganography, intrusion detection, etc.

In January 2002, the Wall Street Journal wrote a lengthy article[1] describing how a WSJ reporter acquired two computers from a looter in Kabul in November 2001, and what the paper found on the computers: 1,750+ text and video files, many of them encrypted. "The looter said he got them from an office al Qaeda abandoned as its Taliban protectors were fleeing Kabul in mid-November … The contents included: A file that names 170 al Qaeda members … a report on a planned operation to 'gather intelligence about American soldiers who frequent nightclubs' along the United States-Canada border … **A primer on coding and encryption of documents. Other files outline procedures for transmitting messages via Pakistan** … a message to Taliban leader Mullah Mohammed Omar … [urging] that the next target be the United Nations …"

There was also a report on a scouting mission that appears to nearly mirror the travels of Richard Reid, the "shoe bomber", although the name identifying the operative who conducted the mission differs – Abdul Ra-uff. The WSJ article says that U.S. intelligence officials who reviewed the materials on the computers "believe that 'Abdul Ra'uff's true identity 'may well be' Reid."

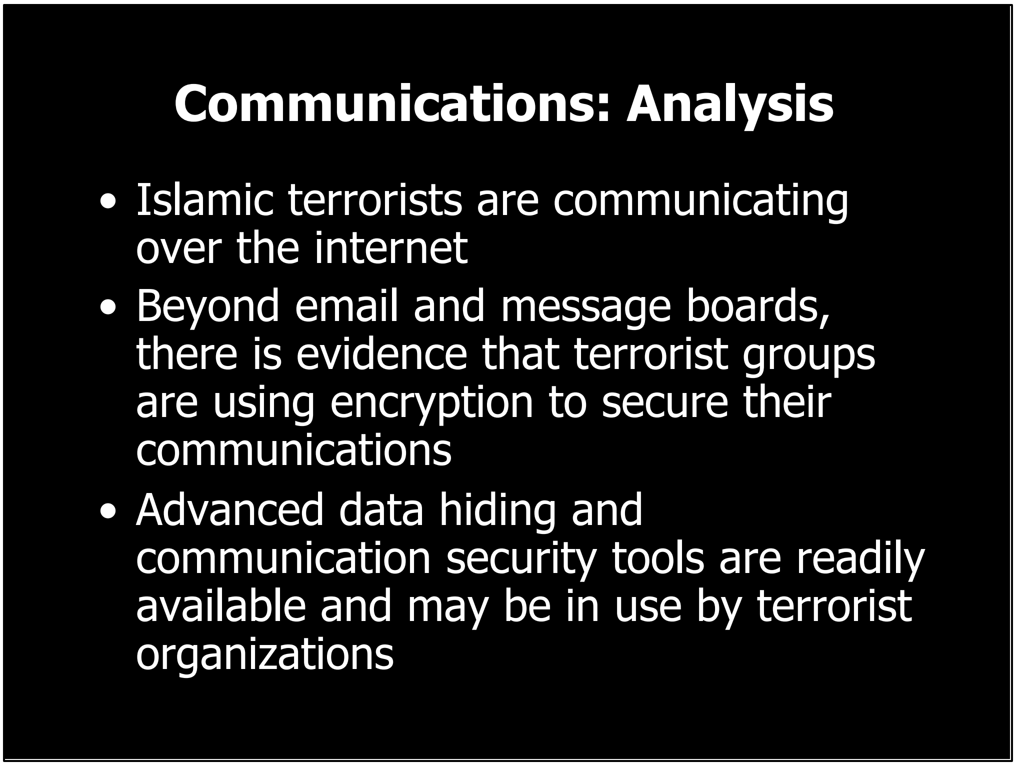
Further reinforcing the reality that Islamic terrorists heavily use the Internet for clandestine communications, the websites and message boards frequented by jihadi have taken to offering tips on online security, encryption, steganography, proxies and anonymizers, and IDS.

The screenshot in this slide was taken from a popular jihadi message board, and includes helpful tips on which programs to use, what system requirements are needed, and where to find the programs.[2]

[1] <http://www.azstarnet.com/attack/indepth/wsj-terrortour.html> – originally printed in the WSJ, and reprinted online at the Arizona Daily Star

[2] <http://anon.user.anonymizer.com/http://al-mojahedoon.net/vb/>

Slide 38



Communications: Analysis

- Islamic terrorists are communicating over the internet
- Beyond email and message boards, there is evidence that terrorist groups are using encryption to secure their communications
- Advanced data hiding and communication security tools are readily available and may be in use by terrorist organizations

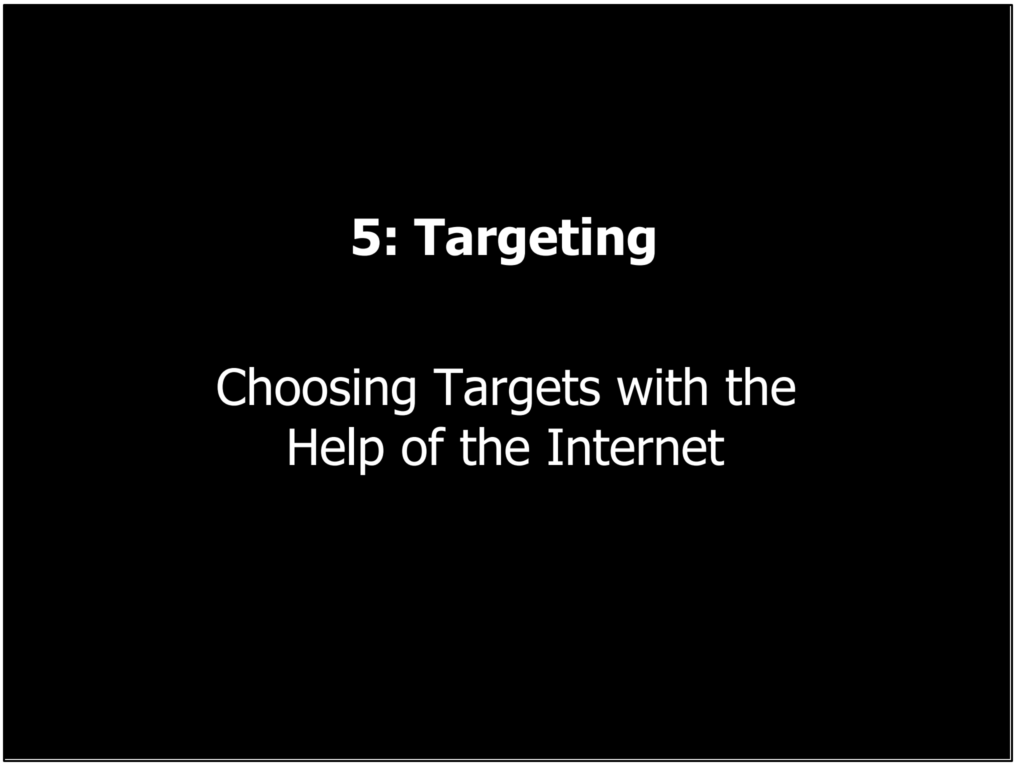
Clearly Islamic terrorists are communicating over the internet using email and message boards as part of their tradecraft.

There is evidence that terrorist groups are using encryption to secure their communications.

Advanced data hiding and communication security tool discussions are found on radical Islamic message boards and are readily available. These technologies may already be in use by terrorist organizations.

The trend in communication is to use information technologies to facilitate terrorist tradecraft.

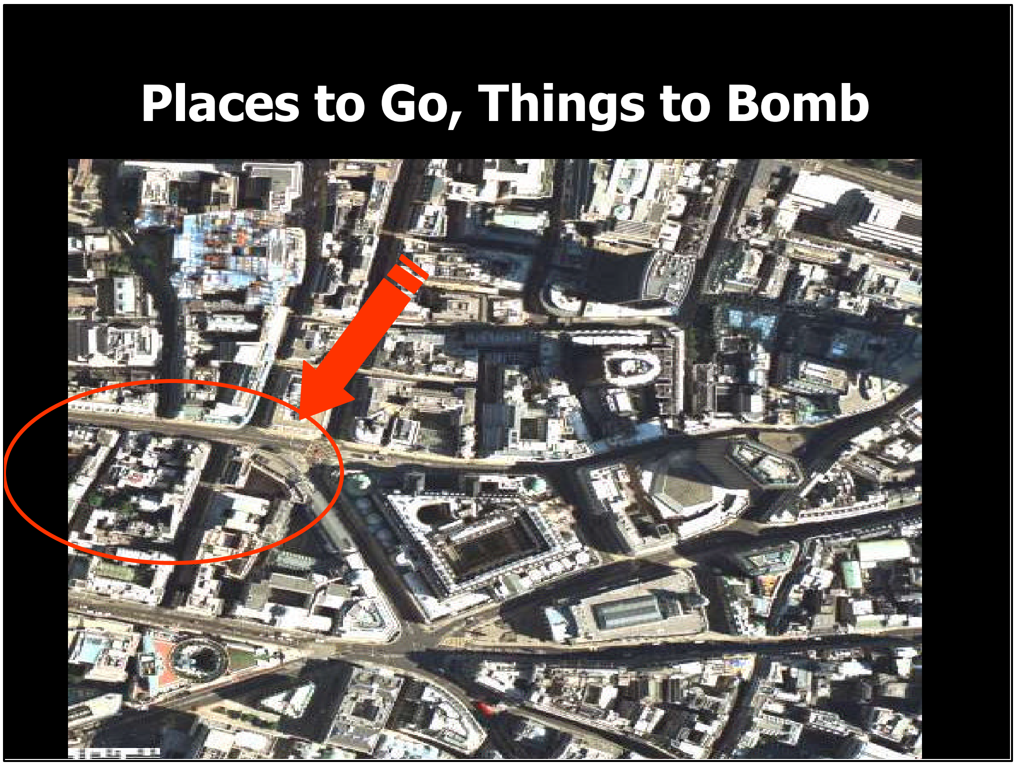
Slide 39



5: Targeting

Choosing Targets with the Help of the Internet

Slide 40

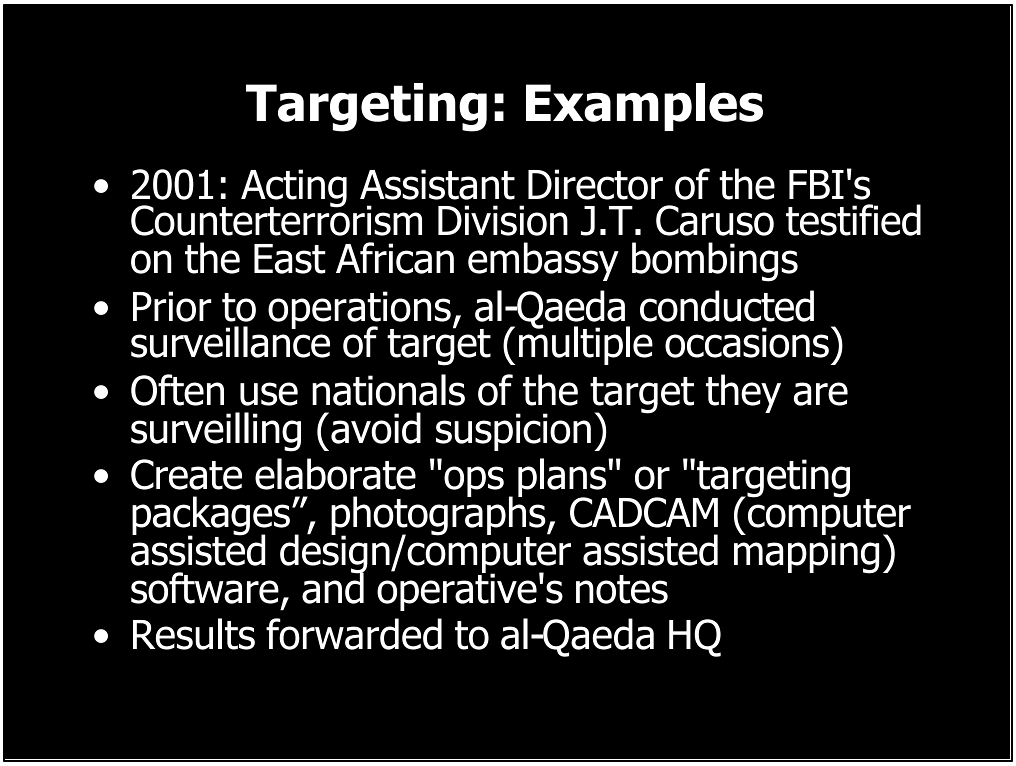


Places to Go, Things to Bomb

Terrorists and their associates have been using computers for years to conduct surveillance and to create targeting packages to submit to leadership for operational approval.

The explosion of public information regarding buildings, people, and organizations, including satellite imagery, has only helped terrorists.

For example, the publicly-available aerial photo above, downloaded in January 2003, is of the London Stock Exchange.[1] The London Stock Exchange might make an extremely attractive target for terrorists, as the business transacted there is a key element in the global economy, a symbol of Western capitalism, and a large physical target located in a major metropolitan area.



Targeting: Examples

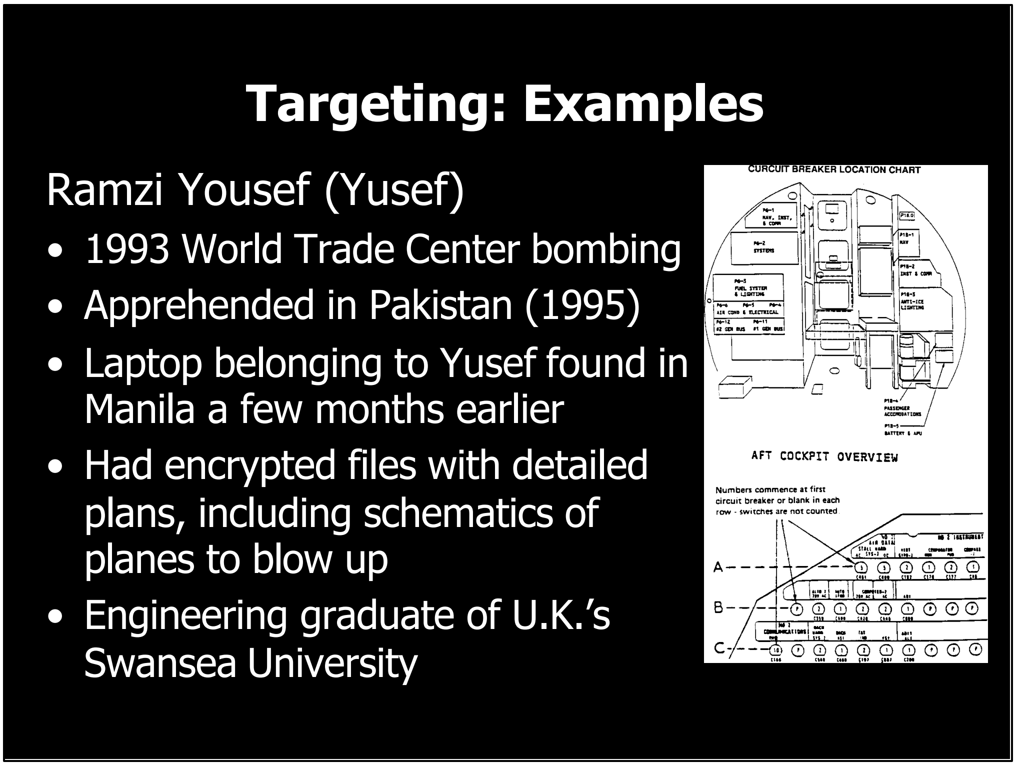
- 2001: Acting Assistant Director of the FBI's Counterterrorism Division J.T. Caruso testified on the East African embassy bombings
- Prior to operations, al-Qaeda conducted surveillance of target (multiple occasions)
- Often use nationals of the target they are surveilling (avoid suspicion)
- Create elaborate "ops plans" or "targeting packages”, photographs, CADCAM (computer assisted design/computer assisted mapping) software, and operative's notes
- Results forwarded to al-Qaeda HQ

In testimony before the Senate Committee on Foreign Relations’ Subcommittee on International Operations and Terrorism (December 18, 2001), J.T. Caruso (Acting Assistant Director of the FBI's Counterterrorism Division) related lessons learned during the East Africa embassy bombing trial.

“Prior to carrying out the operation, Al-Qaeda conducts surveillance of the target, sometimes on multiple occasions, often using nationals of the target they are surveilling to enter the location without suspicion. The results of the surveillance are forwarded to Al-Qaeda HQ as elaborate ‘ops plans’ or ‘targeting packages’ prepared using photographs, CADCAM (computer assisted design/computer assisted mapping) software, and the operative's notes.”[1]

[1] <http://www.fbi.gov/congress/congress01/caruso121801.htm>

Slide 42



Targeting: Examples

Ramzi Yousef (Yusef)

- 1993 World Trade Center bombing
- Apprehended in Pakistan (1995)
- Laptop belonging to Yusef found in Manila a few months earlier
- Had encrypted files with detailed plans, including schematics of planes to blow up
- Engineering graduate of U.K.'s Swansea University

CURCUIT BREAKER LOCATION CHART
AFT COCKPIT OVERVIEW
Numbers commence at first circuit breaker or blank in each row - switches are not counted
A
B
C

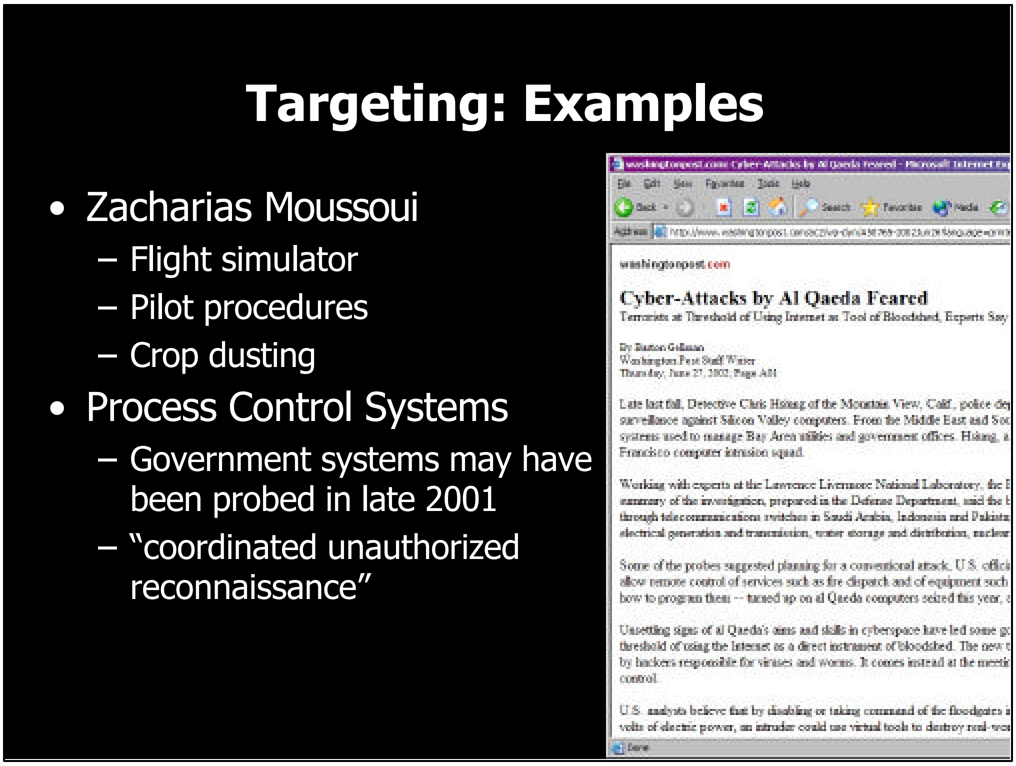
Testimony in 1998 by then-Director of the FBI Louis Freeh (before the Senate Select Committee on Intelligence) confirmed that even in the early to mid-1990s, Middle Eastern terrorists were making extensive use of computers to store and transfer information.

Freeh's testimony states "[Ramzi] Yousef's laptop computer, which was seized in Manila, contained encrypted files […]." [1] Yousef is the high-level AQ operative who masterminded the 1993 World Trade Center bombing.

Bomb-making equipment that was in the apartment started a fire and the computer got left behind. Yousef sent an associate back to get the computer, but the associate was picked up by the police. The laptop computer had encrypted files that contained extensive details of his various plans, including details of airplanes he planned to blow up. Reportedly, some of the encryption Yousef used was so complex, it took upwards of two years before U.S. authorities discovered what was in some of the files.

An interesting note: Yousef has a degree in engineering from Swansea University, United Kingdom.

[1] <http://www.techlawjournal.com/congress/crypto/80128fbi.htm> – (this link has just the excerpted testimony pertaining to encryption)



Targeting: Examples

- Zacharias Moussoui
  - Flight simulator
  - Pilot procedures
  - Crop dusting
- Process Control Systems
  - Government systems may have been probed in late 2001
  - “coordinated unauthorized reconnaissance”

washingtonpost.com Cyber-Attacks by Al Qaeda Feared - Microsoft Internet Ex
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Done

washingtonpost.com

Cyber-Attacks by Al Qaeda Feared

Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say

By Barton Gellman
Washington Post Staff Writer
Thursday, June 27, 2002; Page A01

Late last fall, Detective Chris Hsiung of the Mountain View, Calif., police de
surveillance against Silicon Valley computers. From the Middle East and So
systems used to manage Bay Area utilities and government offices. Hsiung, a
Francisco computer intrusion squad.

Working with experts at the Lawrence Livermore National Laboratory, the
summary of the investigation, prepared in the Defense Department, said the
through telecommunications switches in Saudi Arabia, Indonesia and Pakista
electrical generation and transmission, water storage and distribution, nuclea

Some of the probes suggested planning for a conventional attack, U.S. offici
allow remote control of services such as fire dispatch and of equipment such
how to program them -- turned up on al Qaeda computers seized this year,

Unsettling signs of al Qaeda's aims and skills in cyberspace have led some g
threshold of using the Internet as a direct instrument of bloodshed. The new
by hackers responsible for viruses and worms. It comes instead at the meeti
control.

U.S. analysts believe that by disabling or taking command of the floodgates
volts of electric power, an intruder could use virtual tools to destroy real-wo

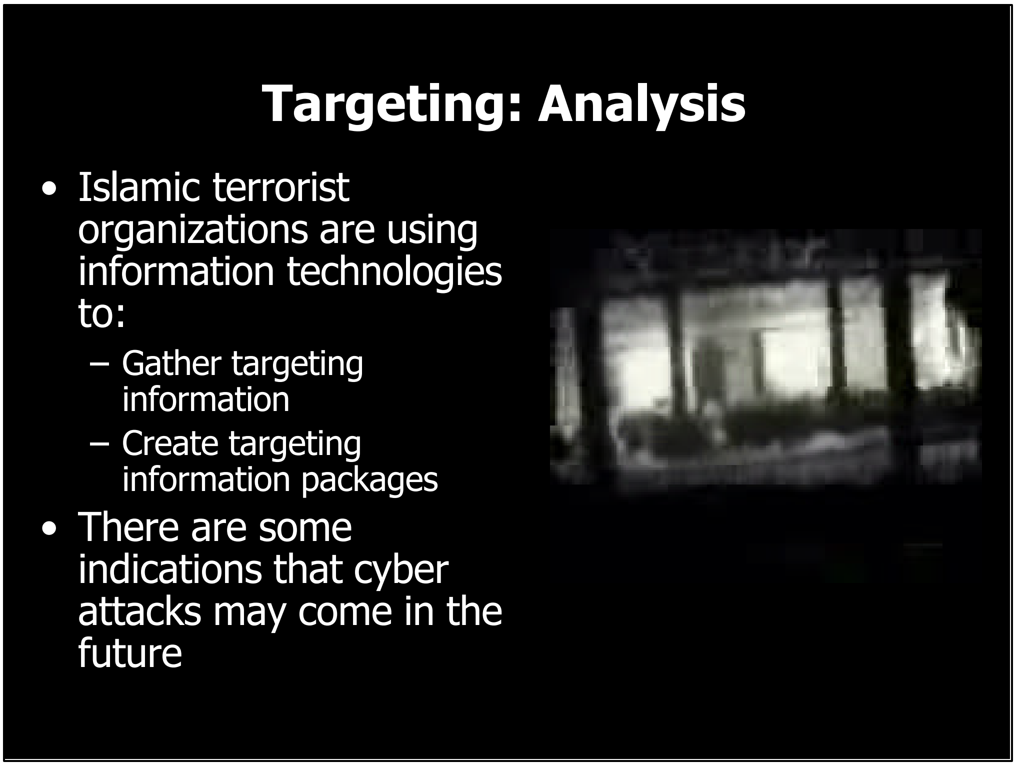
In the indictment against Zacharias Moussaoui, it states that Moussaoui had among his possessions a flight simulator program, software for reviewing pilot procedures for a Boeing 747 Model 400, and a computer disk of information on aerial spraying of pesticides. The indictment also outlines Moussaoui’s use of e-mail to inquire about flight training.[1]

There is additional evidence that cyber targets may be on the terrorists’ list. According to a Washington Post article [2] by Barton Gelman, a number of computer systems for public utilities and other governmental systems in CA and throughout the country were the target of coordinated unauthorized reconnaissance in late 2001, apparently originating in the Middle East and South Asia. The report states:

“Some of the probes suggested planning for a conventional attack, U.S. officials said. But others homed in on a class of digital devices that allow remote control of services such as fire dispatch and of equipment such as pipelines. More information about those devices -- and how to program them -- turned up on al Qaeda computers seized this year, according to law enforcement and national security officials. Unsettling signs of al Qaeda's aims and skills in cyberspace have led some government experts to conclude that terrorists are at the threshold of using the Internet as a direct instrument of bloodshed ... Most significantly, perhaps, U.S. investigators have found evidence in the logs that mark a browser's path through the Internet that al Qaeda operators spent time on sites that offer software and programming instructions for the digital switches that run power, water, transport and communications grids. In some interrogations, the most recent of which was reported to policymakers last week [June 2002], al Qaeda prisoners have described intentions, in general terms, to use those tools.”

[1] <http://www.fbi.gov/pressrel/speeches/mous/pdf> & [2]

Slide 44



Targeting: Analysis

- Islamic terrorist organizations are using information technologies to:
  - – Gather targeting information
  - – Create targeting information packages
- There are some indications that cyber attacks may come in the future

Islamic terrorist organizations are using information technologies to:

1. Gather targeting information and
2. Create targeting information packages

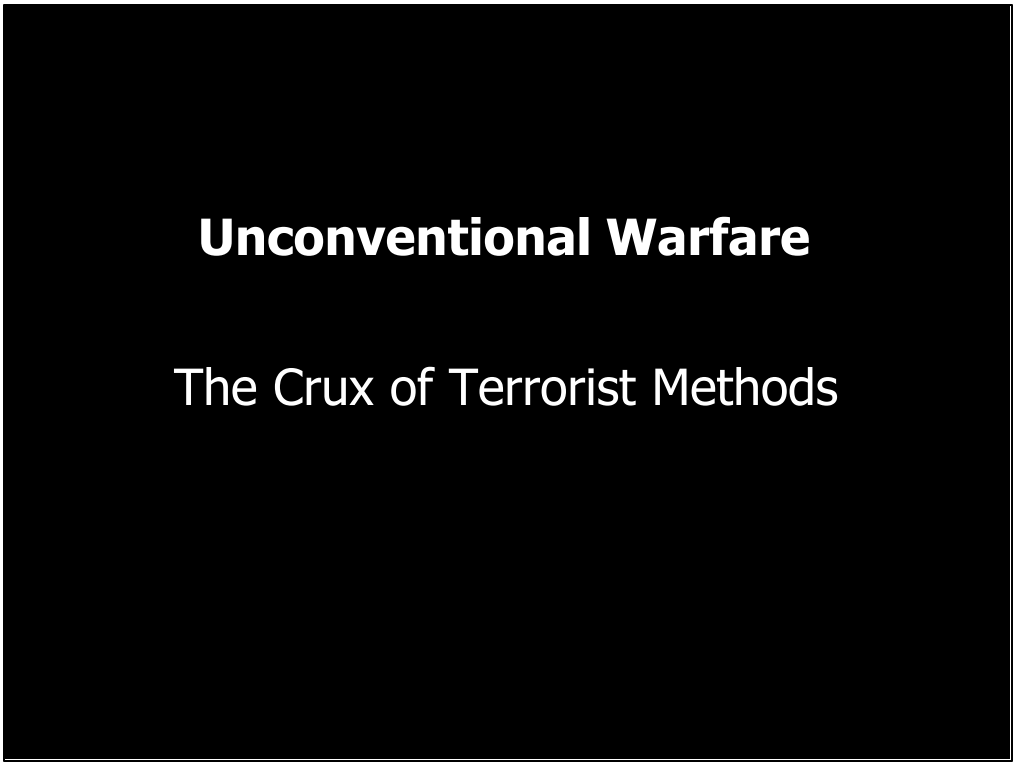
The video on this slide is a excerpt from the "19 Lions" propaganda video that portrayed the September 11th hijackers preparing for the attack.

You can clearly see the use of information technologies by the attackers. It must be noted that often these scenes are staged.

The information found on computer hard drives and in the hands of Islamic terrorists leads us to believe that there are subtle indications that cyber attacks may come in the future.

The final section of this presentation examines how Islamic terrorists may use cyber technologies for unconventional attacks.

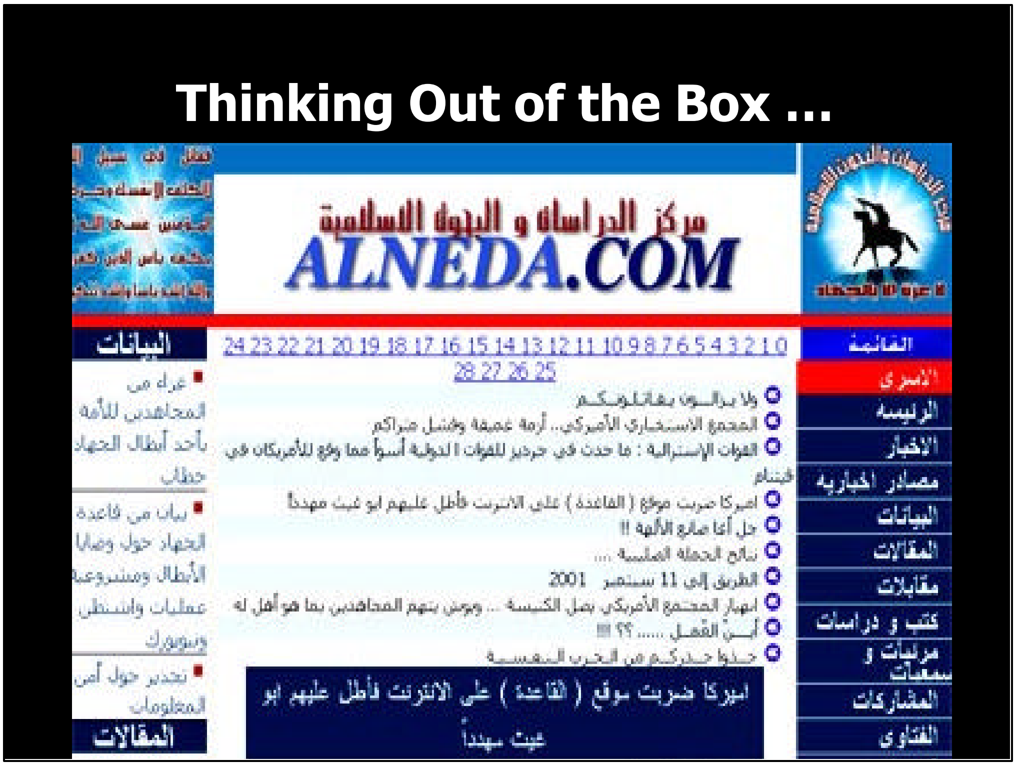
Slide 45



Unconventional Warfare

The Crux of Terrorist Methods

Slide 46



Thinking Out of the Box ...

مركز الدراسات و البحوث الاسلامية
ALNEDA.COM

القائمة
الأسرى
الرئيسه
الأخبار
مصادر اخباريه
البيانات
المقالات
مقابلات
كتب و دراسات
مرئيات و سمعيات
المشاركات
الفتاوى

24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
28 27 26 25

- ولا يزالـون يقاتلونكـم
- المجمع الاستخباري الأمريكي.. أزمة عميقة وفشل متراكم
- القوات الإسترالية : ما حدث في جرديز للقوات الدولية أسوأ مما وقع للأمريكان في شاهي كوت
- امريكا ضربت موقع (القاعدة) على الانترنت فأطل عليهم ابو غيث مهدداً
- حل أنا صانع الآلهة !!
- نتائج الحملة الصليبية ....
- الطريق إلى 11 سبتمبر 2001
- انهيار المجتمع الأمريكي يصل الكنيسة .. وبوش يتهم المجاهدين بما هو أهل له
- أيـن الفعـل ...... ؟؟ !!!
- خـذوا حـذركـم من الحرب النفسيـة

امريكا ضربت موقع (القاعدة) على الانترنت فأطل عليهم ابو غيث مهدداً

البيانات
- عزاء من المجاهدين للأمة بأحد أبطال الجهاد خطاب
- بيان من قاعدة الجهاد حول وصايا الأبطال ومشروعية عمليات واشنطن ونيويورك
- تحذير حول أمن المعلومات
المقالات

The hacker wars between pro-Palestinian and pro-Israeli groups are well-documented in open media sources.[1] Pakistani/Kashmiri supporters and Indian hackers have perpetuated a very similar conflict for several years.[2, 3] Although to date there have been no publicly known incidents of cyber attacks specifically conducted by al-Qaeda, there has been considerable speculation about the possibility of al-Qaeda making use of unconventional warfare techniques. Although some critics have commented that this is unlikely, it is dangerous to assume that simply because no cyber attack directly attributable to a terrorist group is known to have happened yet, such an attack will not happen. In fact history has proven that one of the classic mistakes that militaries make is "fighting the last war".

Vince Cannistraro, former chief of counterterrorism at the CIA (in a November 2002 Computerworld article), indicated that "… many Islamic fundamentalists, some of them close to al-Qaeda, have developed expertise in computer science. 'And some are well schooled in how to carry out cyberattacks,' Cannistraro said. 'We know from material retrieved from [al-Qaeda] camps in Afghanistan that this is true.' " [4] In this section we will look at jihadists' and jihad sympathizers' use of technology in the context of unconventional attacks.

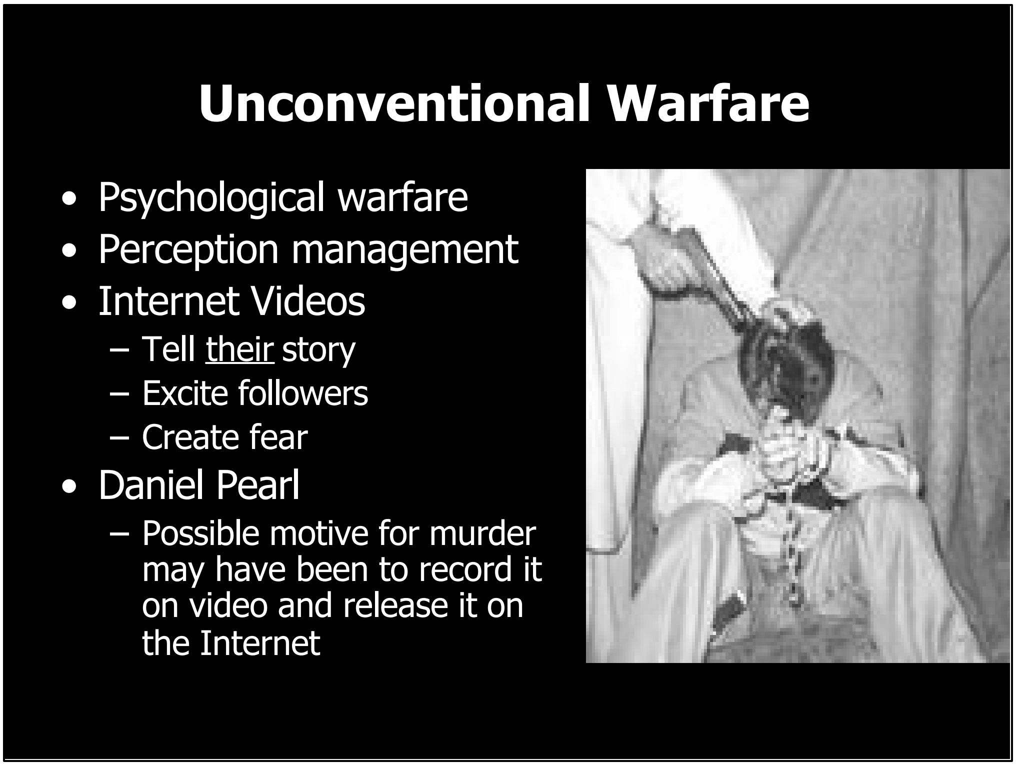
[1] <http://www.wired.com/news/politics/0,1283,40030,00.html>

[2] <http://www.hvk.org/articles/0501/93.html>

[3] <http://www.wired.com/news/politics/0,1283,41048,00.html>

[4]<http://www.computerworld.com/governmenttopics/government/itgovernment/story/0,10801,76150,00.html>

Slide 47



Unconventional Warfare

- Psychological warfare
- Perception management
- Internet Videos
  - Tell their story
  - Excite followers
  - Create fear
- Daniel Pearl
  - Possible motive for murder may have been to record it on video and release it on the Internet

Chechen separatists and their sympathizers have a reputation for maintaining extensive video and photographic records of their activities.[1] As we saw earlier in the presentation these resources offer significant value to their propaganda, recruitment, and training activities. By maintaining their own image records, Islamic terrorists can continue to tell the story they want to tell, not just what the media chooses to tell. There are suggestions, too, that audio and video files of Islamic terrorist leadership have been doled out to the public with great strategic care, with precisely-timed releases to whip up followers and to panic Westerners.

A theory on possible Islamists' strategic use of technology in an unconventional fashion was outlined in Jane's Intelligence Review, in an August 2002 article by Paul Eedle.[2] In the article, Eedle puts forth the notion that AQ has a deliberate strategy with regard to videotaping their activities. "Al-Qaeda's use of the internet and videotapes demonstrate[sic] that 'perception management' is central to the conduct of its war with the West. In fact, it is possible to view all of Al-Qaeda's operations – including acts of violence – as one vast perception management operation. Everything Al-Qaeda does is taped to use later … An important motive for the murder of US journalist Daniel Pearl in Pakistan may well have been to produce the horrific video of one of his kidnappers mutilating his body, which was posted on the internet in May."[3]

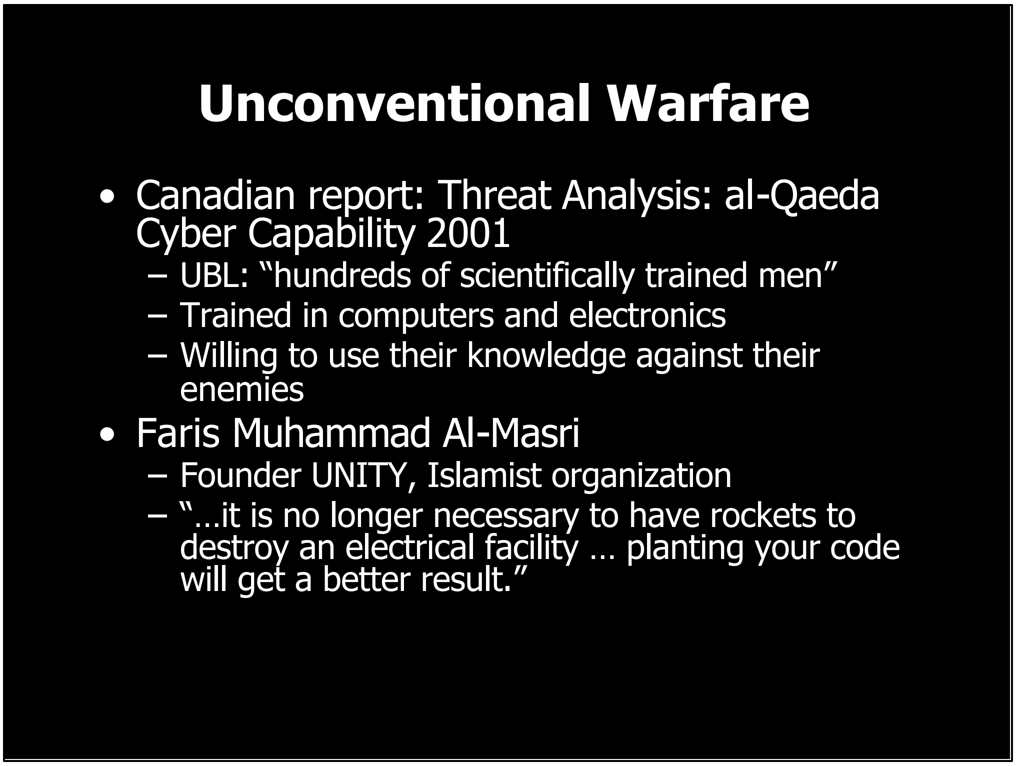
Is the same true about the information Islamic terrorist leaders are revealing about their cyber capabilities?

[1] Paul Eedle, "Al-Qaeda takes fight for 'hearts and minds' to the web", Jane's Intelligence Review, August 2002, pp. 24-26.

[2] Ibid, p. 26.

[3] Chechen separatist/mujahideen website, <http://www.kavkazcenter.com>, has a large library of video clips for download – includes many, many clips of operations against Russian troops, unfolding in real time – blowing up buildings, personnel carriers, even a successful SAM launch against a Russian helicopter.

Slide 48



Unconventional Warfare

- Canadian report: Threat Analysis: al-Qaeda Cyber Capability 2001
  - UBL: “hundreds of scientifically trained men”
  - Trained in computers and electronics
  - Willing to use their knowledge against their enemies
- Faris Muhammad Al-Masri
  - Founder UNITY, Islamist organization
  - “…it is no longer necessary to have rockets to destroy an electrical facility … planting your code will get a better result.”

A threat analysis conducted by Canada’s Office of Critical Infrastructure Protection and Emergency Preparedness (“Threat Analysis: Al-Qaida Cyber Capability”, November 2, 2001[1]) says that bin Laden himself claimed to have hundreds of scientifically and technically trained men, specifically including those trained in computers and electronics, who were willing to die for their cause and to use their knowledge against their enemies.

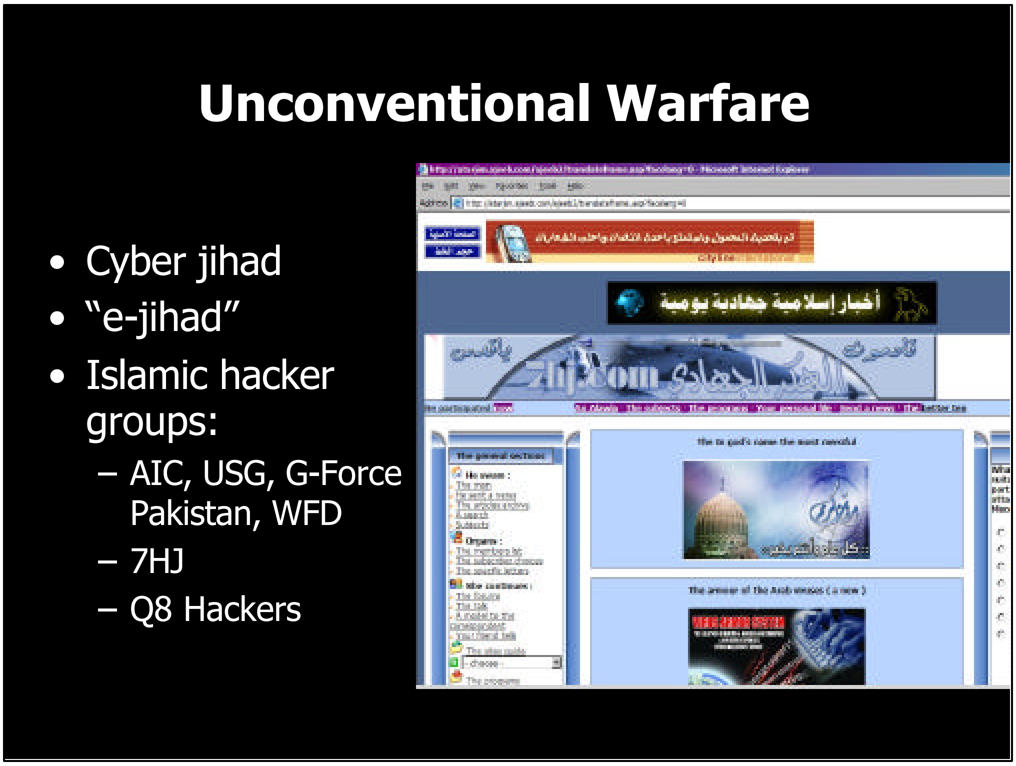
Giles Norman of IT-Director.com, in his April 2002 article on the impact of cyberwar on the business sector, quoted Faris Muhammad Al-Masri, founder of UNITY (www.ummah.net/unity), a website with an Islamist ideology : “As information technology comes to rule every part of our life, it is no longer necessary to have rockets to destroy an electrical facility. Instead, penetrating the enemy's networks and planting your code will get a better result.”[2]

So we see that Islamic terrorist leaders are touting their cyber capabilities, but do they really have them at their disposal?

[1] <http://www.ocipep-bpiepc.gc.ca/opsprods/other/TA01-001_E.asp>

[2] <http://www.it-director.com/article.php?id=2744>

Slide 49



Unconventional Warfare

- Cyber jihad
- "e-jihad"
- Islamic hacker groups:
  - AIC, USG, G-Force Pakistan, WFD
  - 7HJ
  - Q8 Hackers

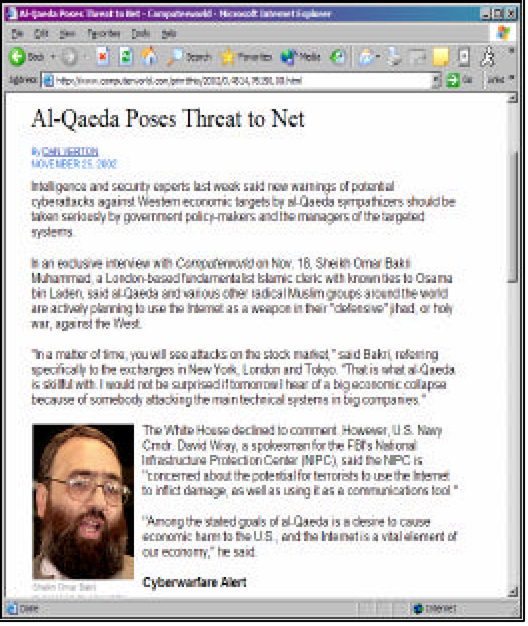
To answer the question, we can turn in part to historical analysis. A number of Islamic fundamentalist hacker groups have been very active in the past few years, including the Anti-India Crew (AIC), the Unix Security Guards (USG), G-Force Pakistan, and the World's Fantabulous Defacers (WFD). According to a report by a British firm called mi2g, which has collected a database of more than 6,000 hacker entities and 30,000 hacking incidents, these groups and others have launched extensive denial-of-service attacks and web defacements on Israeli, American, and Indian targets.[1] There are "e-jihad" (sometimes seen as "e-jehad") and "cyber-jihad" websites run by and devoted to Muslim and Arabic hackers and aspiring hackers, including 7hj.7hj.com, www.q80hackers.com (pronounced "Kuwaiti"), www.arabhackers.org,_and arabhackerz.8m.com. Many of these sites are focused on attacking a certain set of targets, such as Israeli sites or Indian sites, but these groups widely share information on techniques and tools, all the while espousing the same fundamentalist rhetoric as the more political or militaristic jihadi sites. There is at least one (and possibly more) site that automatically downloads a hacker tool to any user who enters the site (www.geocities.com/baitab2af/), although the tools can be readily mitigated with anti-virus software and other tactics. Some of these hacker tools include: DeepThroat, BackOrifice, SubSeven, and IP Stealer. These tools are all listed in an area of the Arabic-language site promoting "e-jihad". From this data we can see there are definable groups of Islamic sympathizers at least purporting to have technical skills that would facilitate cyber attacks.

[1] <http://www.mi2g.com/cgi/mi2g/press/180602.php>

Slide 50

Unconventional Warfare

- Omar Bakri Muhammed – November 2002
  - you will see attacks on the stock market
  - New York, London and Tokyo
  - economic collapse because of somebody attacking the main technical systems in big companies



Al-Qaeda Poses Threat to Net

By DAN VERTON
NOVEMBER 25, 2002

Intelligence and security experts last week said new warnings of potential cyberattacks against Western economic targets by al-Qaeda sympathizers should be taken seriously by government policy-makers and the managers of the targeted systems.

In an exclusive interview with Computerworld on Nov. 18, Sheikh Omar Bakri Muhammad, a London-based fundamentalist Islamic cleric with known ties to Osama bin Laden, said al-Qaeda and various other radical Muslim groups around the world are actively planning to use the Internet as a weapon in their "defensive" jihad, or holy war, against the West.

"In a matter of time, you will see attacks on the stock market," said Bakri, referring specifically to the exchanges in New York, London and Tokyo. "That is what al-Qaeda is skillful with. I would not be surprised if tomorrow I hear of a big economic collapse because of somebody attacking the main technical systems in big companies."

The White House declined to comment. However, U.S. Navy Cmdr. David Wray, a spokesman for the FBI's National Infrastructure Protection Center (NIPC), said the NIPC is "concerned about the potential for terrorists to use the Internet to inflict damage, as well as using it as a communications tool."

"Among the stated goals of al-Qaeda is a desire to cause economic harm to the U.S., and the Internet is a vital element of our economy," he said.

Cyberwarfare Alert

In perhaps the most publicized event indicating Islamic terrorist and supporter intentions with regard to cyber attacks, Omar Bakri Muhammed (one of the U.K.'s three most prominent and controversial Islamist clerics, and leader of Al Muhajiroun) granted an exclusive interview to Computerworld in November 2002.[1,2]

In this interview, Mr. Bakri made direct statements that AQ has specifically trained on and is planning to use cyber attack techniques against economic targets. " 'In a matter of time you will see attacks on the stock market,' Mr. Bakri said, referring specifically to the markets in New York, London, and Tokyo." The true extent of OBM's actual direct ties and access to insider information from UBL and AQ has been questioned by some (including Vince Cannistraro[2] who called Mr. Bakri "a fire-breather" with no special knowledge of AQ plans – Cannistraro acknowledged AQ's capabilities in cyber attack techniques but went on to say "But their expertise seems mostly dedicated to communicating securely among al-Qaeda cells.") Thus, Mr. Bakri's statements must be considered with a critical eye.

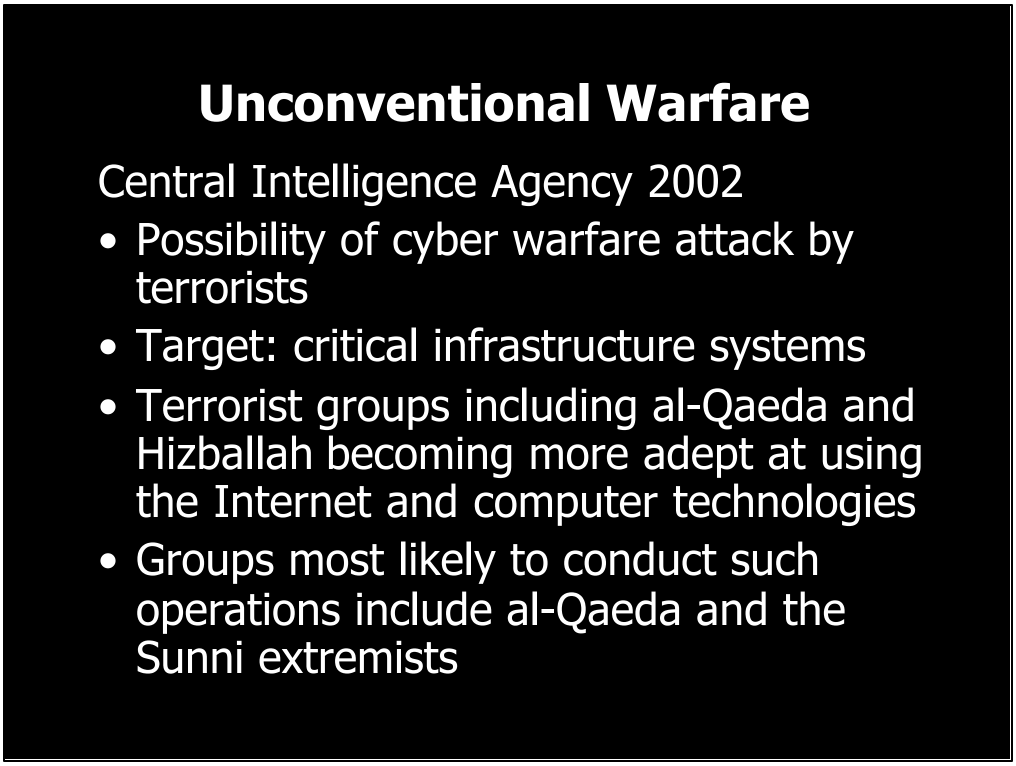
That said, however, there is no doubt that Mr. Bakri leads a group of radically-inclined Islamists who identify themselves with elements of the global Islamic jihad, and who many sources say act as recruiters for the jihad, channeling personnel and funds to terrorist training camps in Afghanistan and Pakistan.

Dan Verton, Computerworld, "Exclusive: Bin Laden associate warns of cyberattacks", November 18, 2002

[1] <http://www.pcworld.com/news/article/0,aid,107052,00.asp>

[2] <http://www.computerworld.com/securitytopics/security/story/0,10801,76000,00.html>

Slide 51



Unconventional Warfare

Central Intelligence Agency 2002

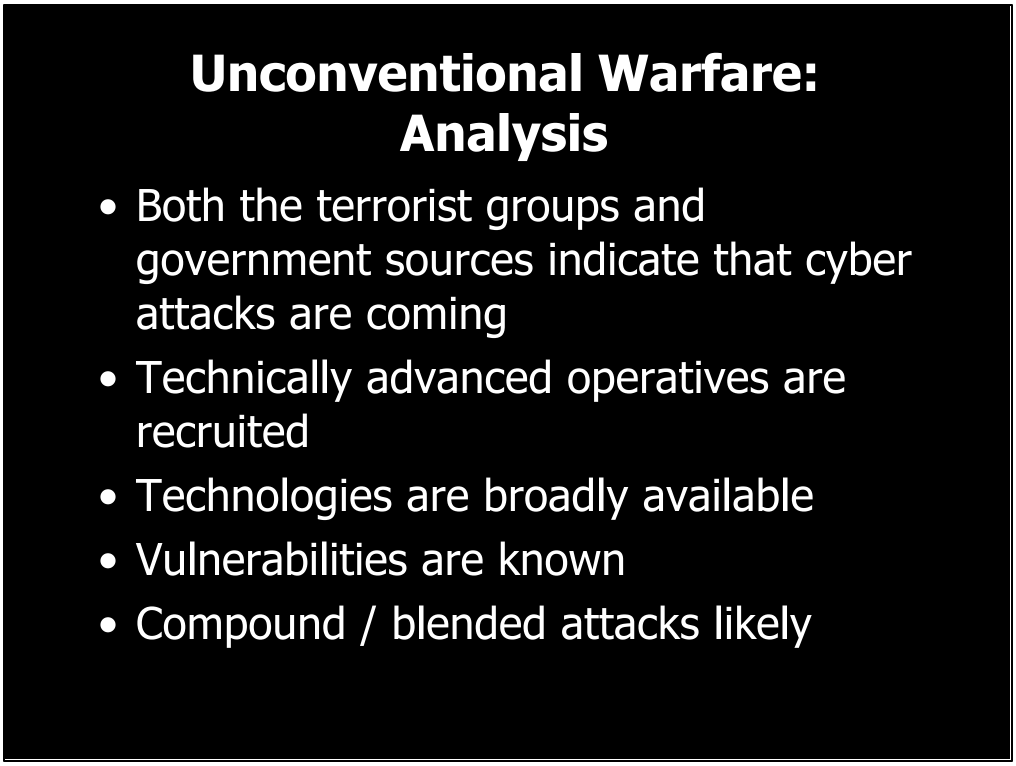
- Possibility of cyber warfare attack by terrorists
- Target: critical infrastructure systems
- Terrorist groups including al-Qaeda and Hizballah becoming more adept at using the Internet and computer technologies
- Groups most likely to conduct such operations include al-Qaeda and the Sunni extremists

So what are our own intelligence and security services saying about Islamic groups' cyber attack capabilities? The Central Intelligence Agency stated in its responses to the "Questions for the Record from the Worldwide Threat Hearing" conducted by the Senate Select Intelligence Committee (April 8, 2002): "We [the CIA] are alert to the possibility of cyber warfare attack by terrorists on critical infrastructure systems that rely on electronic and computer networks.

Cyberwarfare attacks against our critical infrastructure systems will become an increasingly viable option for terrorists as they become more familiar with these targets, and the technologies required to attack them. Various terrorist groups--including al-Qa'ida and Hizballah--are becoming more adept at using the Internet and computer technologies, and the FBI is monitoring an increasing number of cyber threats. The groups most likely to conduct such operations include al-Qa'ida and the Sunni extremists that support their goals against the United States. These groups have both the intentions and the desire to develop some of the cyberskills necessary to forge an effective cyber attack modus operandi." [1]

[1] <http://www.fas.org/irp/congress/2002_hr/020602cia.html>

Slide 52



Unconventional Warfare: Analysis

- Both the terrorist groups and government sources indicate that cyber attacks are coming
- Technically advanced operatives are recruited
- Technologies are broadly available
- Vulnerabilities are known
- Compound / blended attacks likely

Both the terrorist groups and government sources indicate that cyber attacks are coming. As we have seen earlier in the presentation, Islamic terrorist groups are recruiting technically advanced operatives. The technologies needed to launch cyber attacks are broadly available. U.S. cyber vulnerabilities are well known, however the cascading effects of cyber attacks are not well understood.

Slide 53

Conclusion

Making Sense of it All

WALL ST
ON TIME

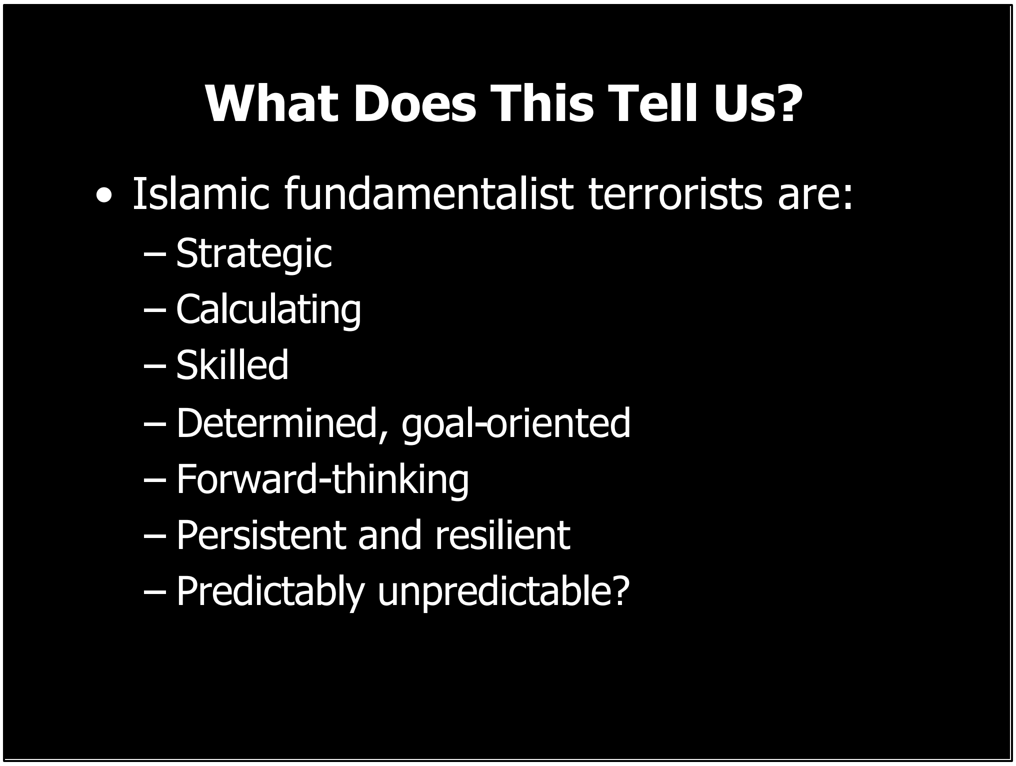
So what does all of this information tell us?

We must take all of the varied pieces and try to weave together a clear understanding of what Islamic fundamentalist terrorists' cyber abilities are, how they use cyber technology, and how they are most likely to use those skills and that knowledge in the future.

We must not fall prey to what many have called a "failure of imagination" in anticipating future threats to our homeland security.

At the same time, it is important that we **not** over-state the threat, or the public may become numb to the warnings if predicted outcomes fail to happen. We need to be vigilant, proactive, and sensible.

Slide 54



What Does This Tell Us?

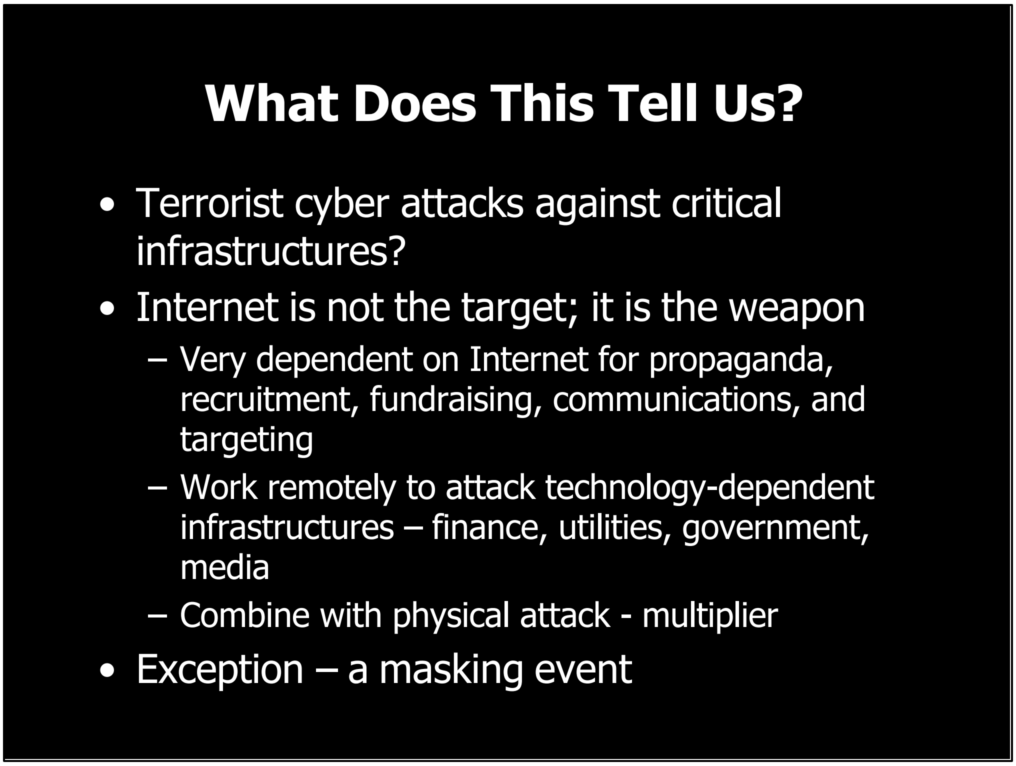
- Islamic fundamentalist terrorists are:
  - Strategic
  - Calculating
  - Skilled
  - Determined, goal-oriented
  - Forward-thinking
  - Persistent and resilient
  - Predictably unpredictable?

What have we specifically learned about cyber capabilities of terrorists engaged in the global Islamic jihad?

We have learned that many are formidable opponents, that they think very strategically, and that they carefully calculate the impact that proposed operations will have. They seek out technically educated recruits, and they train other recruits in specialized skills as needed. We know that they are utterly determined to reach their goals, or die trying. We can see that they are willing to spend years planning operations if they believe that the outcome is worth it. We have also clearly seen that if they are not successful on the first attempt at a target, they are likely to keep coming back until they **are** successful.

They have clearly demonstrated that their far-flung, loosely-networked structure allows them to bounce back, even if localized elements of their operation are severely damaged. And if there is one thing that can probably safely be predicted with certainty about their activities, it is that they are likely to continue to be unpredictable.

Slide 55



What Does This Tell Us?

- Terrorist cyber attacks against critical infrastructures?
- Internet is not the target; it is the weapon
  - Very dependent on Internet for propaganda, recruitment, fundraising, communications, and targeting
  - Work remotely to attack technology-dependent infrastructures – finance, utilities, government, media
  - Combine with physical attack - multiplier
- Exception – a masking event

With regard to Islamic terrorists using cyber attacks against our critical infrastructures, some fairly clear themes emerged from our research. Foremost among these is that terrorists have over the past several years become extremely dependent on the Internet as an operational tool. As demonstrated in this presentation, access to and use of computers and the Internet has allowed Islamic terrorists to share information, to recruit new followers, to raise money, to keep in touch, and to plan operations. As an example, after their Afghani base of operations was largely eliminated, AQ has relied heavily on cyber technology to regroup and to begin carrying out new activities.

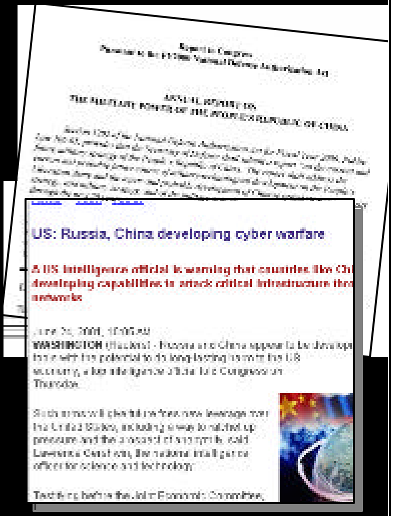
It has also allowed them a voice in the Western world, through the media. For these reasons, it is unlikely that most Islamic terrorists would see any benefit to "bringing down the Internet". It is quite likely, though, that these groups would at least attempt (if they have not already) to use the Internet to attack other critical infrastructures, either as an isolated act or in combination with a physical attack. An example commonly used is a scenario where a chem/bio attack is launched on a city, and simultaneously the city's 9-1-1 emergency communications systems is rendered useless via an electronic attack, fostering panic and disrupting emergency response. It was recently proved that 9-1-1 systems are vulnerable to electronic attack. In January 2003, the SQL or "Slammer" worm completely disrupted the 9-1-1 system for a municipality just outside Seattle, WA.[1] An exception to the prediction that organized terrorists would not want to shut down the Internet would be if they wanted to create a very visible, disruptive event that masked a more covert action.

[1]<http://www.sans.org/alerts/mssql.php>;<http://www.washingtonpost.com/wp-dyn/articles/A46928-2003Jan26.html>;<http://www.cbsnews.com/stories/2003/01/28/tech/main538200.s

Slide 56

Nation States

- Asymmetric warfare to counter U.S. military and economic superiority
- 20-30 states believed to be developing cyber warfare capabilities
- Targeted nation-states will use cyber warfare techniques
- Professional intelligence services



Report to Congress
Pursuant to the FY2000 National Defense Authorization Act

ANNUAL REPORT ON
THE MILITARY POWER OF THE PEOPLE'S REPUBLIC OF CHINA

[illegible]

US: Russia, China developing cyber warfare

A US intelligence official is warning that countries like Chi developing capabilities to attack critical infrastructure thro networks

June 21, 2001, 10:06 AM
WASHINGTON (Reuters) - Russia and China appear to be develop [illegible] with the potential to do long-lasting harm to the US economy, a top intelligence official told Congress on Thursday.

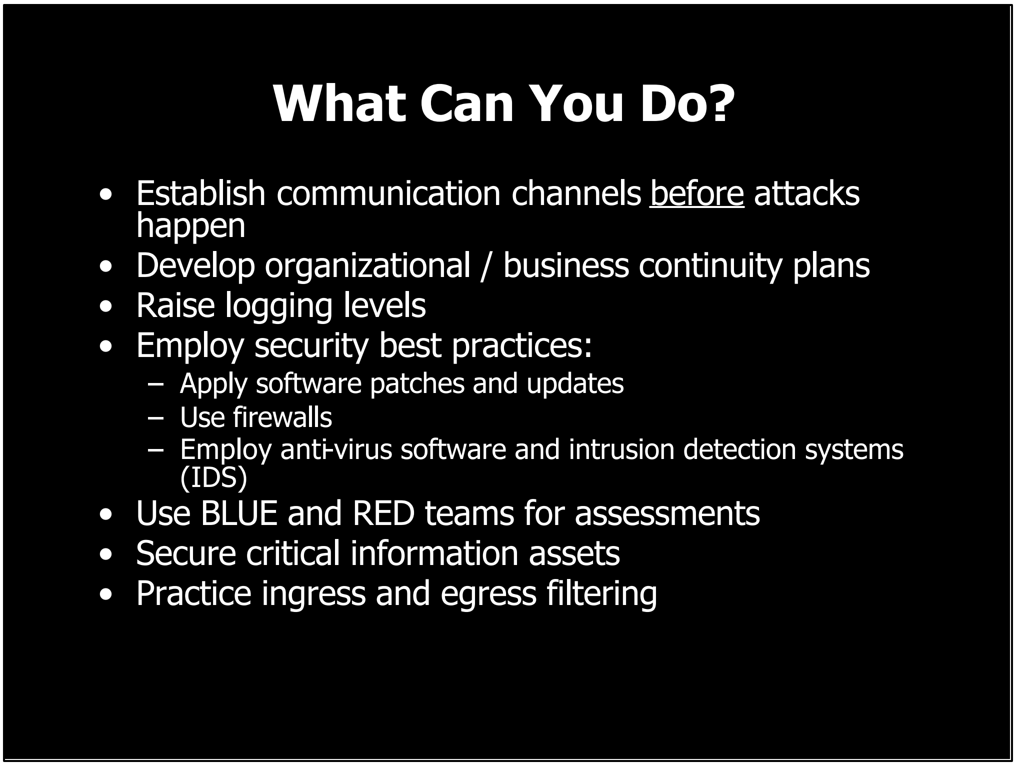
Such arms will give hostile nations new leverage over the United States, including a way to ratchet up pressure and the element of anonymity, said Lawrence Gershwin, the national intelligence officer for science and technology.

Testifying before the Joint Economic Committee,

In 200 John A. Serabian the Information Operations Issue Manager at the Central Intelligence Agency testified before the Joint Economic Committee on Cyber Threats and the U.S. Economy. He commented that “We are detecting, with increasing frequency, the appearance of doctrine and dedicated offensive cyber warfare programs in other countries. We have identified several, based on all-source intelligence information, that are pursuing government-sponsored offensive cyber programs. Foreign nations have begun to include information warfare in their military doctrine, as well as their war college curricula, with respect to both defensive and offensive applications. They are developing strategies and tools to conduct information attacks.”

Significant efforts are currently focused on preventing attacks from terrorist groups however both government officials and media reports indicate several nation states are developing a cyber attack capability to combat overwhelming American conventional military force. Perhaps a greater threat than the terrorist groups are hostile nation states that have the intelligence services, funding, and patience to attack our critical infrastructures over the long run.

Slide 57



What Can You Do?

- Establish communication channels before attacks happen
- Develop organizational / business continuity plans
- Raise logging levels
- Employ security best practices:
  - Apply software patches and updates
  - Use firewalls
  - Employ anti-virus software and intrusion detection systems (IDS)
- Use BLUE and RED teams for assessments
- Secure critical information assets
- Practice ingress and egress filtering

This slide presents some very general actions that each individual who has viewed this presentation can take to harden their infrastructure and be prepared in case of a cyber attack.

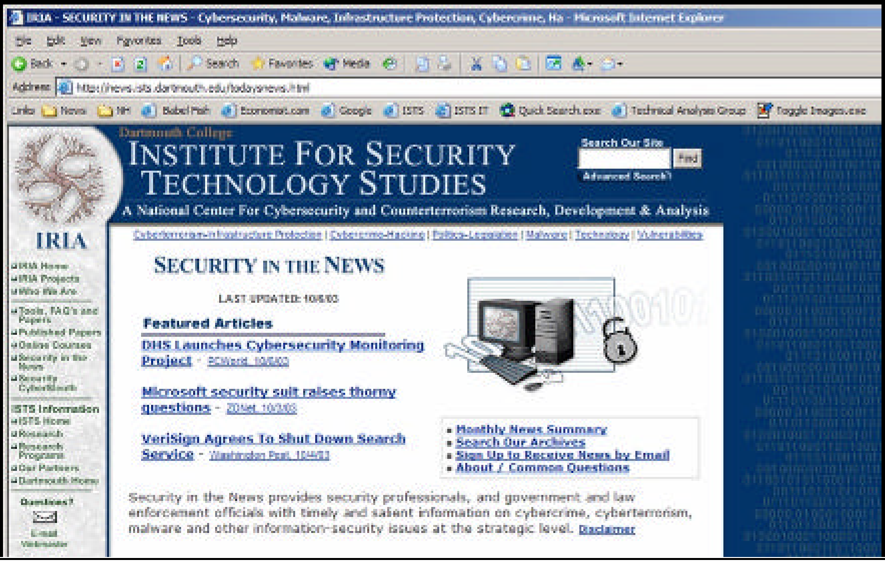
Resources

- Department of Homeland Security
  www.dhs.gov
- USSS Electronic Crime Task Forces
  www.ectaskforce.org
- Institute for Security Technology Studies
  www.ists.dartmouth.edu
- State and Local law enforcement

Slide 59

Resources: Open Source Intelligence

www.ists.dartmouth.edu



IRIA - SECURITY IN THE NEWS - Cybersecurity, Malware, Infrastructure Protection, Cybercrime, Ha - Microsoft Internet Explorer

Address http://news.ists.dartmouth.edu/todaysnews.html

Dartmouth College

INSTITUTE FOR SECURITY TECHNOLOGY STUDIES

A National Center For Cybersecurity and Counterterrorism Research, Development & Analysis

IRIA

SECURITY IN THE NEWS

LAST UPDATED: 10/6/03

Featured Articles

DHS Launches Cybersecurity Monitoring Project - PCWorld, 10/6/03

Microsoft security suit raises thorny questions - ZDNet, 10/3/03

VeriSign Agrees To Shut Down Search Service - Washington Post, 10/4/03

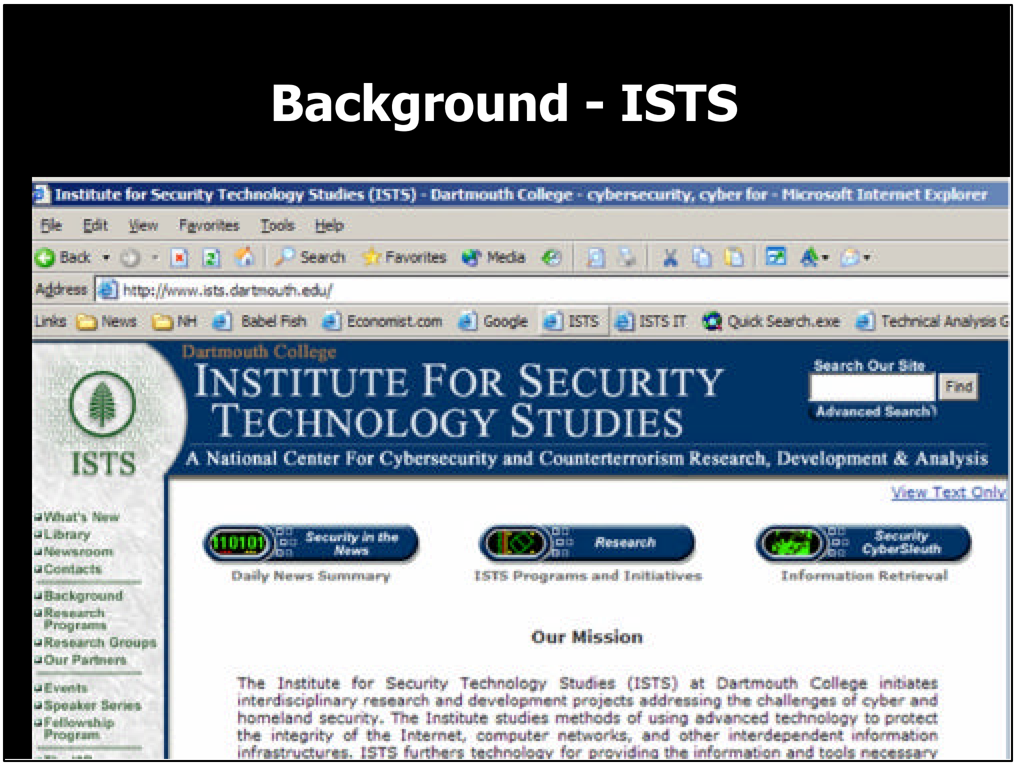
- Monthly News Summary
- Search Our Archives
- Sign Up to Receive News by Email
- About / Common Questions

Security in the News provides security professionals, and government and law enforcement officials with timely and salient information on cybercrime, cyberterrorism, malware and other information-security issues at the strategic level. Disclaimer

File Edit View Favorites Tools Help
Back Search Favorites Media
Links News Google ISTS ISTS IT Quick Search.exe Technical Analysis Group Toggle Images.exe
Search Our Site
Find
Advanced Search?
ISTS Information

The ISTS provided a daily open source intelligence briefing available on the ISTS web site.

Slide 60



Background - ISTS

Institute for Security Technology Studies (ISTS) - Dartmouth College - cybersecurity, cyber for - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.ists.dartmouth.edu/
Links News NH Babel Fish Economist.com Google ISTS ISTS IT Quick Search.exe Technical Analysis G
Dartmouth College
INSTITUTE FOR SECURITY TECHNOLOGY STUDIES
ISTS
A National Center For Cybersecurity and Counterterrorism Research, Development & Analysis
Search Our Site
Find
Advanced Search
View Text Only
What's New
Library
Newsroom
Contacts
Background
Research Programs
Research Groups
Our Partners
Events
Speaker Series
Fellowship Program
110101
Security in the News
Daily News Summary
Research
ISTS Programs and Initiatives
Security CyberSleuth
Information Retrieval

Our Mission

The Institute for Security Technology Studies (ISTS) at Dartmouth College initiates interdisciplinary research and development projects addressing the challenges of cyber and homeland security. The Institute studies methods of using advanced technology to protect the integrity of the Internet, computer networks, and other interdependent information infrastructures. ISTS furthers technology for providing the information and tools necessary

The Institute for Security Technology Studies (ISTS) at Dartmouth College initiates interdisciplinary research and development projects addressing the challenges of cyber and homeland security. The Institute studies methods of using advanced technology to protect the integrity of the Internet, computer networks, and other interdependent information infrastructures. ISTS furthers technology for providing the information and tools necessary to assist communities and first responders with the evolving, complex security landscape. ISTS is a member of and administers The Institute for Information Infrastructure Protection (I3P), a consortium of 24 leading academic institutions, non-profits and federal laboratories that brings industry, academia and government together to articulate and focus on problems that need to be solved to help ensure the nation's information infrastructure is safe, secure and robust.

*** The authors of this report have made every effort to provide original definitions, use definitions provided in past ISTS publications, and acknowledge the sources of publicly available common knowledge definitions integrated into this document. Footnote definitions were compiled from multiple sources in addition to those created by ISTS researchers. Due to the complexity and public availability of many of the technical definitions used in this study, ISTS acknowledges the possibility that one or more definitions may resemble definitions offered in other non-ISTS sources. We invite the authors or readers of these non-ISTS sources to notify ISTS in writing if similar language is found in this document. Upon notification we will takes steps to verify the claim. If appropriate, ISTS will insert language crediting the appropriate non-ISTS source or to change our own definitional language.