



# Ethical Hacking and Countermeasures

Version6



## Module XLIII

Cyber Warfare- Hacking  
Al-Qaida and Terrorism

## Al Qaeda Hacker Attack Scheduled To Begin November 11th

An Israeli news site claims Bin Laden's cyber legions are retaliating against Western surveillance programs.

By Thomas Claburn, [InformationWeek](#)

Nov. 1, 2007

URL: <http://www.informationweek.com/story/showArticle.jhtml?articleID=202800885>

An [Israeli Web site](#) is warning that al Qaeda hackers will attack Western, Jewish, Israeli, Muslim apostate, and Shiite Web sites starting on Sunday, November 11th.

"...al Qaeda is retaliating against Western intelligence agencies' tactics, which detect new terrorist sites and zap them as soon as they appear," reports [DEBKAFfile](#), a news site based in Israel.

"Until now, the jihadists kept dodging the assault by throwing up dozens of new sites simultaneously," the news report said. "This kept the trackers busy and ensured that some of the sites survived, while empty pages were promptly replaced. But as al Qaeda's cyber wizards got better at keeping its presence on the Net for longer periods, so too did Western counter-attackers at knocking them down. Now Bin Laden's cyber legions are fighting back. The electronic war they have declared could cause considerable trouble on the world's Internet."

How disruptive the attack will be has yet to be determined. It's not clear where DEBKAFfile is getting its information and those in the government who worry about such things don't appear to be more worried than usual.

A U.S. Secret Service agent who forwarded the report to a security mailing list cautioned that the news did not constitute an official USSS advisory and a spokesperson for the USSS said, "We didn't send out the bulletin."

Source: <http://www.informationweek.com>

## China accused of cyberattacks on New Zealand

By Liam Tung

[http://www.news.com/China-accused-of-cyberattacks-on-New-Zealand/2100-7348\\_3-6207678.html](http://www.news.com/China-accused-of-cyberattacks-on-New-Zealand/2100-7348_3-6207678.html)

Story last modified Thu Sep 13 11:31:32 PDT 2007

**The New Zealand secret service has suggested the Chinese government was behind attacks on the country's networks.**

New Zealand Prime Minister **Helen Clark** yesterday assured reporters that no classified information had been compromised but confirmed that she believes that foreign-government spies were behind the cyberattack.

While Clark said officials know which government was behind the attack, she would not name the country suspected.

"We have very smart people to provide protection every time an attack is tried. Obviously, we learn from that," she told reporters.

Now on News.com

[Can Motorola regain lost luster?](#) [Google's wireless power play](#) [Cracking open the iPod Touch Extra: Craigslist marriage scheme busted](#)

**Warren Tucker**, New Zealand's Security Intelligence Service director, hinted to local newspaper *The Dominion Post* that the Chinese government was responsible for the attacks, referring to previous allegations about the country's spying activities by Canada's secret service.

The allegations come only a week after the Chinese foreign ministry denied that the Chinese government had endorsed attacks on the computer networks of Germany, **the United States** and the United Kingdom.

"Any accusation of Chinese military force attacking computer systems of foreign governments is groundless, irresponsible and out of ulterior motives," Chinese foreign-ministry representative Jiang Yu said in a recent press conference. "As far as I know, up till now, the Chinese police have not received any request for investigation assistance from the relevant countries."

*Liam Tung of **ZDNet Australia** reported from Sydney.*

Source: <http://www.news.com/>

## How Al-Qaida Site Was Hijacked

Patrick Di Justo  08.10.02 | 2:00 AM

A Maryland hacker used simple Web tools like whois and traceroute -- as well as online translation software and an anti-cybersquatting service -- to take over the domain name of al-Qaida's website. And he's ready to do it again.

Jon Messner, the Internet entrepreneur who perpetrated the recent domain hijacking, used SnapName's [Snapback](#) service to obtain ownership of the domain [www.alneda.com](#).

Since at least March 2001, al-Qaida has been using Al Neda ("The Call") as its official Internet headquarters.

The switch in ownership was made on July 16, after the owners of alneda.com deleted its registration from an ISP in Malaysia. Messner believes this was in preparation to establish Al Neda on another server.

"It was a slippery bastard, but I've got it now," Messner laughs. "I own alneda.com."

Al Neda contained editorials by major al-Qaida leaders, some of them explicit calls for action and justification of terrorist activities. There was a message board, containing relatively innocuous messages believed to be coded signals.

There was also a multimedia section containing pictures, audio files and videos of Osama bin Laden.

Earlier this year, Al Neda was being hosted on a [server farm](#) in Kuala Lumpur. Messner believes the United States government pressured the Malaysians to drop [www.alneda.com](#) from its site a few months ago.

When al-Qaida deleted the domain from Malaysia, Messner struck. "After they pushed it out of the Malaysian registry... in that split second the domain became exposed, and Snapback... put my info in there," Messner said.

Source: <http://www.wired.com/>

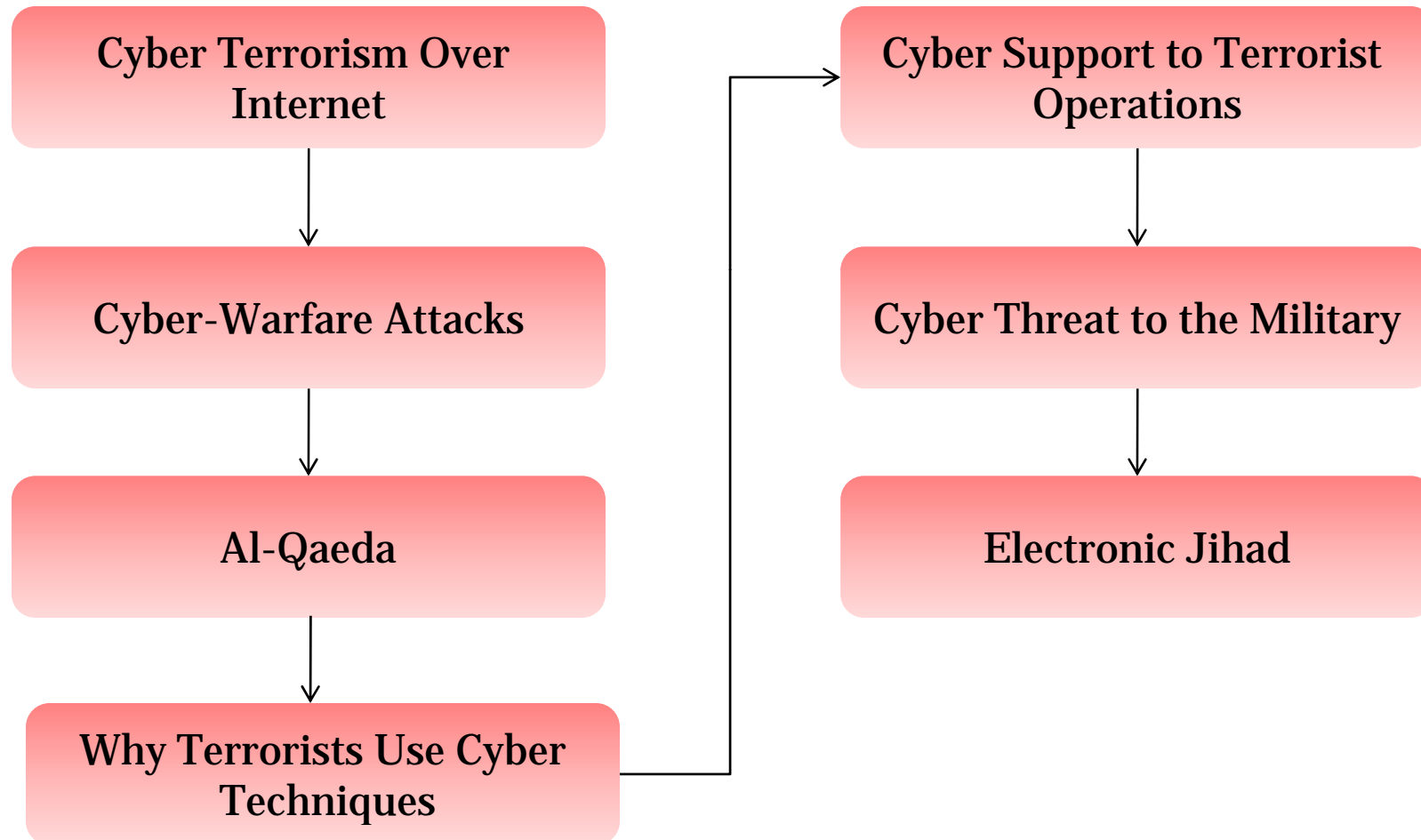
# Module Objective

This module will familiarize you with:

- Cyber Terrorism Over Internet
- Cyber-Warfare Attacks
- Al-Qaeda
- Why Terrorists Use Cyber Techniques
- Cyber Support to Terrorist Operations
- Cyber Threat to the Military
- Electronic Jihad



# Module Flow



# Cyber Terrorism Over Internet



According to <http://www.cybercrimes.net/Terrorism>, FBI defined Cyber terrorism as *“the use of computing resources against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives”*



Cyber-terrorism is the leveraging of a target's computer and information technology, particularly via the Internet, to cause physical, real-world harm, or severe disruption



Cyber terrorism can weaken countries economy; by doing this it can strip the country of its resources and make it more vulnerable to military attack

# Cyber-Warfare Attacks

Computer virus, logic bombs, and Trojan horse attacks

## Cyber Bullying

- It is the use of electronic information and communication devices such as e-mail, instant messaging, text messages, blogs, mobile phones, pagers, instant messages, and defamatory websites to bully or harass the others



## Cyber Stalking

- It is the use of the Internet or other electronic means to stalk someone
- It is used with online harassment and online abuse





# Cyber-Warfare Attacks (cont'd)

## Web vandalism:

- Attacks that deface WebPages, or denial-of-service attacks

## Propaganda:

- Political messages can be spread through or to anyone by accessing Internet

## Gathering data:

- Classified information that is not handled securely can be intercepted and even modified, making espionage possible from other side of the world



# Cyber-Warfare Attacks (cont'd)



## Distributed Denial-of-Service Attacks:

- Large numbers of computers in one country launch a DoS attack against systems in another country

## Equipment disruption:

- Military activities that use computers and satellites for co-ordination are at risk from this type of attack, putting soldiers at risk



## Attacking critical infrastructure:

- Power, water, fuel, communications, commercial, and transportation are all vulnerable to a cyber attack

# 45 Muslim Doctors Planned US Terror Raids

## 45 Muslim doctors planned US terror raids

By John Steele, Crime Correspondent

Last Updated: 2:14am BST 06/07/2007

- [Glasgow airport bomber left suicide note](#)
- [Ties that bind terror car bomb suspects](#)
- [Airport attack doctor was known extremist](#)

A group of 45 Muslim doctors threatened to use car bombs and rocket grenades in terrorist attacks in the United States during discussions on an extremist internet chat site.

Police found details of the discussions on a site run by one of a three-strong "cyber-terrorist" gang.

They were discovered at the home of Younis Tsouli, 23, Woolwich Crown Court in south-east London heard.

One message read: "We are 45 doctors and we are determined to undertake jihad and take the battle inside America.

"The first target which will be penetrated by nine brothers is the naval base which gives shelter to the ship Kennedy." This is thought to have been a reference to the USS John F Kennedy, which is often at Mayport Naval Base in Jacksonville, Florida.



Cyber-terrorists: Tariq Daour, Younis Tsouli and Waseem Mughal

The message discussed targets at the base, adding: "These are clubs for naked women which are opposite the First and Third units."

It also referred to using six Chevrolet GT vehicles and three fishing boats and blowing up petrol tanks with rocket propelled grenades.

Investigators have found no link between the Tsouli chat room and the group of doctors and medics currently in custody over attempted car bomb attacks in London and Glasgow.

However, sources said it was "definitely spooky" that the use of doctors for terrorist purposes was being discussed in jihadi terrorist circles up to three years ago.

Source: <http://www.telegraph.co.uk/>

# Net Attack

## Net Attack

By AARON MANNES and JAMES HENDLER  
June 5, 2007

The age of cyberwar has arrived. The attacks on Estonian government and commercial Web sites following the relocation of a Soviet World War II memorial in Tallinn in late April made news around the world. Yet these were not the only, or even the most significant, such assaults this year.

In February, hackers laid siege to six of the 13 "root servers" that form the backbone of the Internet. Had they succeeded in disabling these servers, the Internet would have ceased to function. Fortunately, only two of the root servers were severely affected, causing only some localized slowdowns. The emerging threat of cyberattacks against vital parts of the global economy highlights the urgent need to protect the Net from criminals.

The attack on Estonia was perhaps more akin to a riot than a military strike. Just as a mob might wreck storefronts, cyberattacks defaced or knocked prominent commercial and government Web sites offline. Similar attacks have accompanied other international political spats. Arab and Israeli hackers attack each other's Web sites, as do Pakistani and Indian hackers. After a South Korean speed skater was disqualified for bumping an American rival during the 2002 Winter Olympics, several strikes apparently originating from South Korea hit U.S. servers.

In all these cases, the hackers can cause email delays and fetter access to targeted Web sites. In Estonia, they prevented the national government from explaining the situation, hampered financial transactions and interfered with telephone systems, which rely in part on the Internet to function.

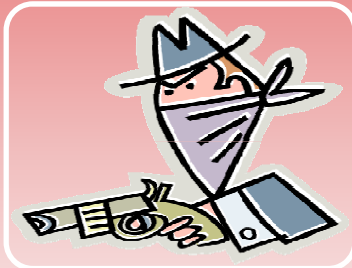
The strikes against the Estonian sites and the Internet root servers are of a type known as Distributed Denial of Service attacks, or DDoS. The assailants begin by installing a virus or other malicious software on a computer, directing it to send messages without its owner's knowledge. These compromised computers, known as bots, are bound together into large networks called botnets. They then simultaneously send messages to the targeted system, overwhelming it and leaving it unable to respond to queries. Low-end estimates indicate that there are tens of millions of bots in the world, and experts have identified some botnets that included more than 100,000 compromised computers.



Source: <http://counterterrorismblog.org/>



Al-Qaeda is an international alliance of Islamic militant organizations founded in 1988



Al-Qaeda has attacked civilian and military targets in various countries; the most notable being the September 11, 2001 attacks that occurred in New York City and Northern Virginia



Characteristic terror techniques include use of suicide attacks and simultaneous bombings of different targets

# Why Terrorists Use Cyber Techniques

The Cyber Division of the FBI states that in the future, cyber-terrorism may become a viable option to traditional physical acts of violence due to:

- Anonymity
- Diverse targets
- Low risk of detection
- Low risk of personal injury
- Low investment
- Operate from nearly any location
- Few resources are needed

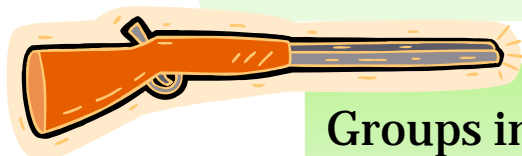


# Cyber Support to Terrorist Operations

Terrorists recognize the benefit of cyber operations and continue to exploit information technology in every function of their operations

Cyber fraud, ranging from credit card theft to money laundering, is the latest wrinkle in terrorists' use of the Internet

Online scams are harder to trace because they are relayed through a sophisticated network of individuals and Web sites worldwide



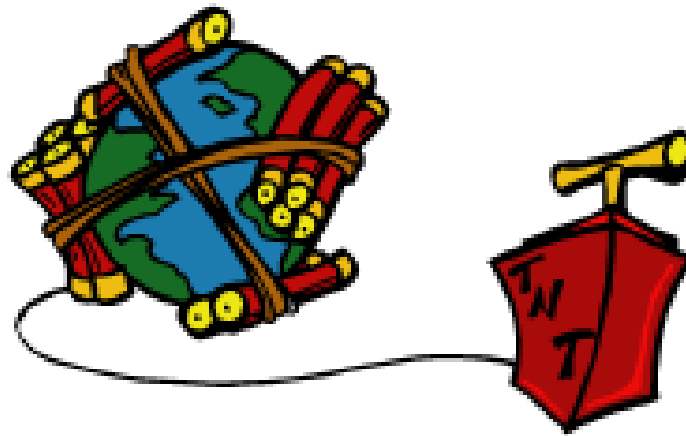
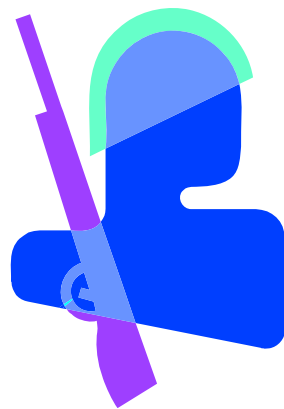
Groups including al-Qaeda use cyberspace for communications, recruiting, and propaganda



# Cyber Support to Terrorist Operations (cont'd)

These operations include:

- Planning
- Recruitment
- Research
- Propaganda







Terrorists use the cyber infrastructure to plan attacks, communicate with each other, and posture for future exploitation

Using steganography, they hide instructions, plans and pictures for their attacks in pictures and posted comments in chat rooms

The images and instructions can only be opened using a “private key” or code known only to the recipients

# Recruitment

Recruitment is the life-blood of a terrorist organization and they use multiple methods to entice new members



In addition to traditional methods, such as written publications, local prayer leaders, audio-video cassettes and CDs promoting their cause; terrorist groups use their own websites to recruit new members



Terrorists provide their view of the history of their organization, its cause, and additional information to encourage potential members to join

Terrorists can tap into thousands of databases, libraries, and newsgroups around the world to gather information on any subject that they need to research

The information can be in the form of text, maps, satellite images, pictures, or even video material

The use of search engines, such as Google, have made searching the Internet very easy and allows terrorists to obtain critical information

Al Qaeda training manual recovered in Afghanistan states:

- “Using public sources openly and without resorting to illegal means, it is possible to gather at least 80% of information about the enemy.”

Terrorists use propaganda to discredit their enemy while making themselves look good

These groups post articles supporting their agendas on these sites, which make them instantly available to the worldwide cyber community

Terrorists make use of propaganda to enlist the support of their own public for jihad and to demoralize the enemy

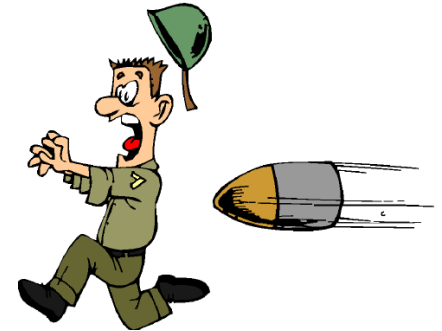


# Cyber Threat to the Military

Military is linked together through the Global Information Grid, computers, and computer networks

Terrorists think that the military is the only vulnerability to command and control systems

A major threat to the military deals with the fact that a large percentage of the Global Information Grid is dependent upon commercial telecommunications links and the Internet, which are not controlled by DOD (Department of Defense)



# Cyber Threat to the Military (cont'd)

Terrorists can hack the following information:

- Commercial transactions
- Payrolls
- Sensitive research data
- Intelligence
- Operational plans
- Procurement sensitive source selection data
- Health records
- Personnel records
- Weapons systems maintenance records
- Logistics operations



# Russia 'hired botnets' for Estonia Cyber-War

## Russia 'hired botnets' for Estonia cyber-war

Russian authorities accused of collusion with botnet owners

Iain Thomson, vnunet.com 31 May 2007

The Russian authorities have been accused of buying time on illegal botnets to launch a denial-of-service attack against Estonia.

The Asymmetric Threats Contingency Alliance (ATCA), which comprises arms groups and financial services companies, claims to have uncovered evidence of alleged collusion between Russia and the botnet owners.

ATCA said that the botnets were only rented for a short period to boost the number of attacking computers to over a million.

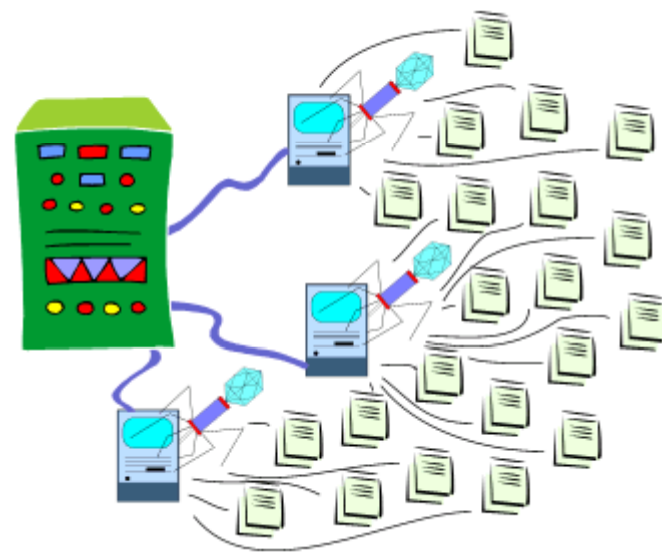
Russia has consistently denied any involvement in the attacks.

"The attackers used a giant network of enslaved computers on 9 May, perhaps as many as one million in places as far away as North America and the Far East, to amplify the impact of their assault," ATCA stated.

"In a sign of their financial resources, there is evidence that [Russia] rented time from trans-national criminal syndicates on botnets.

"On 10 May, it appears that the attackers' time on the rented servers expired, and the botnet attacks fell off abruptly."

ATCA claims that the denial-of-service attacks used very large packets of information streams to clog government websites, banks and newspapers.



Source: <http://www.itnews.com.au/>



# NATO Threatens War with Russia

## NATO Threatens War With Russia

by [James Dunnigan](#)

June 3, 2007

[Discussion Board on this DLS topic](#)

NATO is being called on, by one of its members, to declare Cyber War on Russia. Russia is accused of causing great financial harm to Estonia via Cyber War attacks, and Estonia wants this sort of thing declared terrorism, and dealt with. NATO has agreed to discuss the issue and make a decision. That's big progress in this area.

Cyber Wars have been going on for over a decade now, and they are getting worse. It started in the 1990s, as individuals attacked the web sites in other nations because of diplomatic disputes. This was usually stirred up by some international incident. India and Pakistan went at it several times, and Arabs and Israelis have been trashing each others web sites for years. The Arabs have backed off somewhat, mainly because the Israeli hackers are much more effective. Chinese and Taiwanese hackers go at each other periodically, and in 2001, Chinese and American hackers clashed because of a collision off the Chinese coast between an American reconnaissance aircraft and a Chinese fighter.

In the last two years, these Cyber Wars have escalated from web site defacing and shutting down sites with massive amounts of junk traffic (DDOS attacks), to elaborate espionage efforts against American military networks. The attackers are believed to be Chinese, and some American military commanders are calling for a more active defense (namely, a counterattack) to deal with the matter.



Source: <http://www.strategypage.com/>



# Bush on Cyber War: 'a subject I can learn a lot about'

Original URL:

[http://www.theregister.co.uk/2007/06/26/bush\\_soothes\\_estonians\\_on\\_cyber\\_war/](http://www.theregister.co.uk/2007/06/26/bush_soothes_estonians_on_cyber_war/)

## Bush on cyber war: 'a subject I can learn a lot about'

By [Lewis Page](#)

Published Tuesday 26th June 2007 11:35 GMT

When the presidents of the USA and Estonia met on Monday, cyber warfare was still very much on the Estonian agenda.

Estonia has recently cooled its jets somewhat on the issue of the serious DDoS attacks it suffered in recent months. Initially, the Estonian Government suggested that the Russian Government had mounted a purposeful digital assault, leading to a wave of wide-eyed "cyber-war!" headlines in the Western media.

But Estonia is a NATO member, and no one else in the alliance wanted to hear about a Russian attack on a member state. That would have to be treated as a Russian attack on them all, and so the other nations might have had to respond. Relations with Russia are [fraught enough](#) ([http://www.theregister.co.uk/2007/06/02/putin\\_says\\_star\\_wars\\_phantom\\_menace/](http://www.theregister.co.uk/2007/06/02/putin_says_star_wars_phantom_menace/)) as it is, without an added internet scuffle.

Once Estonia calmed down and adopted a new position - that the DDoS attacks were "terrorist" or "criminal" in nature - NATO was [quite happy to rally round with offers of assistance](#) ([http://www.theregister.co.uk/2007/06/15/cyber\\_war\\_screaming\\_fist/](http://www.theregister.co.uk/2007/06/15/cyber_war_screaming_fist/)), though nothing terribly concrete.

Source: <http://www.theregister.co.uk/>

# E.U. Urged to Launch Coordinated Effort Against Cybercrime

## E.U. urged to launch coordinated effort against cybercrime

By Paul Meller, IDG News Service, 05/22/07

Russia's coordinated attacks against Estonia's computer systems earlier this month were cited as one of the many reasons why the European Union countries should work more closely to fight cybercrime, European Commissioner for Justice and Home Affairs Franco Frattini said Tuesday.

Similarly, the existence of two known criminal gangs operating in the E.U. and believed to have yielded profits in excess of US\$100 million each from Internet fraud is another reason the European Commission -- the E.U.'s executive body -- has decided to take action, the commissioner said in a press conference.

Estonia was temporarily crippled by the Russian attack, which is believed to have been in response to the removal of a Soviet war memorial from the center of the Estonian capital, Tallinn. Estonian officials said the attacks on the country's government Web sites were traced to Russian government servers.

The development of the Internet and other information systems has opened many new possibilities for criminals, the Commission said in a statement issued Tuesday.

"Legislation and operational law enforcement have obvious difficulties in keeping pace," it said. The Commission added that the cross-border character of these threats "further underlines the need for strengthened international cooperation and coordination," not only among national authorities but with countries outside the European Union.

The Commission will host a cybercrime conference in Brussels in November. "The aim, simply, is the eradication of cybercrime," Frattini said.

Sponsored by:

YOUR DATA IS DOUBLING  
EVERY 18 MONTHS.

WHERE DO YOU  
STORE IT ALL?



Tame your data with the HP StorageWorks  
All-In-One Storage Systems



Source: <http://www.networkworld.com/>

# Budget: Eye on Cyber-Terrorism Attacks

## Budget: Eye on cyber-terrorism attacks

By [Munir Kotadia](#), ZDNet Australia

May 08, 2007

URL: <http://www.zdnet.com.au/news/security/soa/Budget-Eye-on-cyber-terrorism-attacks/0,130061744,339276008,00.htm>

The federal government has allocated more than AU\$12 million over the next four years to expand the Australian Government Computer Emergency Readiness Team (GovCERT) and fight high tech crimes, including "cyber-terrorism".

According to federal Attorney-General Philip Ruddock, GovCERT will be enhanced in order to "provide owners and operators of Australia's critical infrastructure with information to help reduce the risks from sophisticated electronic attacks and to provide government with information about the electronic risks to critical infrastructure."

The funding -- allocated from [this year's federal budget](#) -- will also help ensure information is shared in a quick and effective way by government and critical infrastructure organisations.

In addition, a "cyber-exercise program" is in the works to help the country cope with "cyber-terrorism attacks".

"It is imperative that we remain one step ahead of emerging e-threats. The measures announced in this year's budget will help create a secure and trusted operating environment that will benefit all Australians," Ruddock said.

GovCERT was formed over two years ago and at the time, it was [heavily criticised by Graham Ingram](#), director of the Australian Computer Emergency Response Team (AusCERT), for duplicating his organisation's role and wasting taxpayers' money.

Ingram said: "If AusCERT didn't exist, the cost to the government would be estimated at somewhere between AU\$5 million and AU\$10 million a year...The wise move is to support AusCERT because the costs of not doing it are enormous".



Source: <http://www.zdnet.com.au/>

# Cyber Terror Threat is Growing, Says Reid

## Cyber terror threat is growing, says Reid

By George Jones, Political Editor

Last Updated: 2:55am BST 27/04/2007

- **Analysis:** Al-Qa'eda's electronic 'ammunition'
- **Joshua Rozenberg:** Why we must back our judges over Home Office split
- **Pressure mounts for terror leaks inquiry**
- **Sketch:** Angry Cameron demands to be told where Blair gets his leaks
- **Audio:** Leak jibes sting Blair

Terrorists could attempt to cause economic chaos or plane crashes in an electronic attack on the UK's computer networks John Reid, the Home Secretary, said yesterday.

Mr Reid's warning of the "devastating consequences" of cyber terrorism came as he said the reshaping of the Home Office would enable him to "wake up and think about the security of the nation first and foremost every morning".

The Home Office is to be split on May 9, to concentrate on crime reduction, terrorism and mass migration, with Mr Reid directly accountable for assisting the Prime Minister in co-ordinating the Government's security strategy.

Mr Reid said priority was being given to protecting what he described as the country's critical national infrastructure from terrorist attack.

He said al-Qa'eda's aim was to "bleed us to bankruptcy", by attempting to "cripple" financial markets. Western energy supplies were among targets threatened by the terrorist group.

advertisement

While attacks on oil supplies would cause "incalculable damage", Mr Reid said there was now an additional threat of a terrorist assault on the West's 21st century electronic communication systems.

According to the US Federal Bureau of Investigation, cyber terrorism is any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents". A cyber terrorist attack is designed to cause physical violence or extreme financial harm.



Cyber terrorism could target air traffic control systems

Source: <http://www.telegraph.co.uk/>

# Terror Web 2.0

## Terror Web 2.0

### The Net-Centric Operations of Terrorist Groups Today

By Guest Contributor Jeffrey Carr

The latest phase of the Internet revolution, which has been widely referred to as Web 2.0, has not been overlooked by web-based terror networks. A recent study by the Artificial Intelligence Lab of the University of Arizona details precisely how these net-savvy terrorists are using the Web for fund-raising, recruitment, propaganda, logistical support, communications, training, and even cyber warfare.



Source: <http://analysis.threatswatch.org/>

# Table 1: How Websites Support Objectives of terrorist/Extremist Groups

Table 1: How Websites Support Objectives of Terrorist/Extremist Groups <sup>1</sup>		
Terrorist objectives	Tasks supported by web sites	Web features
Enhance communication	<ul style="list-style-type: none"> <li>• Composing, sending, and receiving messages</li> <li>• Searching for messages, information, and people</li> <li>• One-to-one and one-to-many communications</li> <li>• Maintaining anonymity</li> </ul>	<ul style="list-style-type: none"> <li>• Synchronous (chat, video conferencing, MUDs, MOOs) and Asynchronous (e-mail, bulletin board, forum, Usenet newsgroup)</li> <li>• GUI</li> <li>• Help function</li> <li>• Feedback form</li> <li>• Login</li> <li>• E-mail address for webmaster, organization contact</li> </ul>
Increase fund raising	<ul style="list-style-type: none"> <li>• Publicizing need for funds</li> <li>• Providing options for collecting funds</li> </ul>	<ul style="list-style-type: none"> <li>• Payment instruction and facility</li> <li>• E-commerce application</li> <li>• Hyperlinks to other resources</li> </ul>



# Table 1: How Websites Support Objectives of terrorist/Extremist Groups (cont'd)

Terrorist objectives	Tasks supported by web sites	Web features
Diffuse propaganda	<ul style="list-style-type: none"> <li>• Posting resources in multiple languages</li> <li>• Providing links to forums, videos, and other groups' web sites</li> <li>• Using web sites as online clearinghouses for statements from leaders</li> </ul>	<ul style="list-style-type: none"> <li>• Content management</li> <li>• Hyperlinks</li> <li>• Directory for documents</li> <li>• Navigation support</li> <li>• Search, browsable index</li> <li>• Free web site hosting</li> <li>• Accessible</li> </ul>
Increase publicity	<ul style="list-style-type: none"> <li>• Advertising groups' events, martyrs, history, ideologies</li> <li>• Providing groups' interpretation of the news</li> </ul>	<ul style="list-style-type: none"> <li>• Downloadable files</li> <li>• Animated and flashy banner, logo, slogan</li> <li>• Clickable maps</li> <li>• Information resources</li> </ul>
Overcome obstacles from law enforcement and the military	<ul style="list-style-type: none"> <li>• Send encrypted messages via e-mail, forums, or post on web sites</li> <li>• Move web sites to different servers so they are protected</li> </ul>	<ul style="list-style-type: none"> <li>• Anonymous e-mail accounts</li> <li>• Password-protected or encrypted services</li> <li>• Downloadable encryption software</li> <li>• E-mail security</li> <li>• Stenography</li> </ul>

# Table 1: How Websites Support Objectives of terrorist/Extremist Groups (cont'd)

Terrorist objectives	Tasks supported by web sites	Web features
Diffuse propaganda	<ul style="list-style-type: none"> <li>• Posting resources in multiple languages</li> <li>• Providing links to forums, videos, and other groups' web sites</li> <li>• Using web sites as online clearinghouses for statements from leaders</li> </ul>	<ul style="list-style-type: none"> <li>• Content management</li> <li>• Hyperlinks</li> <li>• Directory for documents</li> <li>• Navigation support</li> <li>• Search, browsable index</li> <li>• Free web site hosting</li> <li>• Accessible</li> </ul>
Increase publicity	<ul style="list-style-type: none"> <li>• Advertising groups' events, martyrs, history, ideologies</li> <li>• Providing groups' interpretation of the news</li> </ul>	<ul style="list-style-type: none"> <li>• Downloadable files</li> <li>• Animated and flashy banner, logo, slogan</li> <li>• Clickable maps</li> <li>• Information resources</li> </ul>
Overcome obstacles from law enforcement and the military	<ul style="list-style-type: none"> <li>• Send encrypted messages via e-mail, forums, or post on web sites</li> <li>• Move web sites to different servers so they are protected</li> </ul>	<ul style="list-style-type: none"> <li>• Anonymous e-mail accounts</li> <li>• Password-protected or encrypted services</li> <li>• Downloadable encryption software</li> <li>• E-mail security</li> <li>• Stenography</li> </ul>



# Table 1: How Websites Support Objectives of terrorist/Extremist Groups (cont'd)

Provide recruitment and training	<ul style="list-style-type: none"> <li>• Hosting martyrs' speeches, stories, multi-media that are used for recruitment</li> <li>• Using flashy logos, banners, cartoons to appeal to sympathizers with specialized skills &amp; similar views</li> <li>• Build massive and dynamic online libraries of training resources</li> </ul>	<ul style="list-style-type: none"> <li>• Interactive services (games, cartoons, maps)</li> <li>• Online registration process</li> <li>• Directory</li> <li>• Multi-media</li> <li>• FAQ, alerts</li> <li>• Virtual community</li> </ul>
----------------------------------	--	---

The Pentagon has recently announced that it monitors over 5,000 jihadist sites and keeps a close watch on the top 100 most active and hostile. The European Union launched its "Check the Web" portal in May, 2007, which is a Europol (European Police) resource that all 27 member states can contribute intelligence to. In spite of these efforts, and those conducted by the U.S. Intelligence Community, there are a number of obstacles that confound our ability to find, capture, and evaluate this data.

For one, conventional search engines like Google only crawl and index a tiny amount of the data on the Web; typically the first 101k of a web page. The key words entered into Google's search window are run against the indexed data in Google's massive data stores, rather than the Web itself. For another, terrorist websites may utilize other means to make themselves invisible to web crawlers, including (but not limited to):

- Password-protected pages
- Noindex metatag
- Firewalls
- Relational databases
- Spider traps
- Real-time content

## Table 1: How Websites Support Objectives of terrorist/Extremist Groups (cont'd)

Most researchers involved in the study of the Terror Web understand the limitations of public search engines and resort to the manual collection, storage, and analysis of web content. Qin (Qin et al 2007) points out that a manual form of collection and analysis is very limiting, and that as of November, 2006, almost no studies have been done (Qin et al 2007) which analyze the level of technical sophistication as compared to mainstream organizations.

The Terror Web's capability for cyber warfare was recently demonstrated by the Denial-of-Service attack launched against the government of Estonia, which was a collective world-wide effort by a group of Russian nationalists to disrupt and cripple Estonia's Internet resources. The attack was successful, and required nothing in the way of sophisticated equipment or specialized knowledge. The sheer number and size of bot networks is hard to measure but recent FBI activity, such as Operation Bot Roast, suggests that potential victims of botnet activity could number in the millions. These are just the networks that law enforcement can identify.

It is important to understand that Western governments are fighting a desperate battle to get a handle on these developments. While both service-specific and joint doctrine on how to fight in cyberspace exists, the institutions, policies and procedures necessary to overcome cyber-based terrorist attacks face numerous challenges. Many of these are simply bureaucratic in nature while others are clearly linked to the infrastructure limitations and security measures levied on defense and intelligence agencies. The sooner such limitations can be overcome, the sooner we can effectively counter terrorism in cyberspace.

Thanks to an increase in terrorism research funding made available by various government agencies, there is a growing body of work available from institutions such as RAND, the Centre for the Study of Terrorism and Political Violence at St. Andrews University, Scotland, The Center for Strategic and International Studies (Washington, D.C.), and the Dark Web Project at the University of Arizona, which recently published "Mapping the contemporary terrorism research domain" in October, 2006.

*Jeffrey Carr participated in law enforcement and intelligence gathering activities with the U.S. Coast Guard until 1990. Today he is an information architect for analyst software, and writes about Data Fusion and Geospatial Intelligence at his blog [www.IntelFusion.net](http://www.IntelFusion.net).*

# Electronic Jihad

Electronic Jihad software is used to let the owner of a computer give control of his system to creator of e-Jihad

The makers of e-Jihad can then use a network of “zombies” to attack web sites and other Internet servers

After installing e-Jihad, the user is asked for a username and password that is sent to a central web server

If the user does not have a username yet, he/she can register a new one; he/she can even enter the username of the person who invited him to e-Jihad



# Electronic Jihad (cont'd)

Electronic Jihad Program is a part of long-term vision jihadi Web site Al-jinan.org to use the Internet as a weapon

Electronic Jihad allows users to target specific IP addresses for attack in order to take any servers running at those IP addresses offline

Application includes a Windows-like interface that lets users choose from a list of target Web sites provided via the Al-jinan site, select an attack speed (weak, medium, or strong), and the click on the "attack" button

The attacks from jihadists are interested in taking Web sites down and disrupting economies that they do not like

# Electronic Jihad: Screenshot



# Electronic Jihad' App Offers Cyber Terrorism for the Masses



## 'Electronic Jihad' App Offers Cyberterrorism For The Masses

U.S. businesses would be greatly impacted by any large-scale cyberattacks because most of that infrastructure is run by companies in the private sector.

By Larry Greenemeier, [InformationWeek](#)

July 2, 2007

URL: <http://www.informationweek.com/story/showArticle.jhtml?articleID=200001943>

Although [cyberterrorism](#) has been around since the Internet reached the mainstream more than a decade ago, a relatively new Web-based application offers Islamic jihadis a way for even the relatively nontechnical to target and attack Web sites perceived to be anti-Islamic.

The "Electronic Jihad Program" is part of the long-term vision jihadi Web site [Al-jinan.org](#) has to use the Internet as a weapon, something that affects any organization that relies on the Web.

Electronic Jihad allows users to target specific IP addresses for attack in order to take any servers running at those IP addresses offline. The application even includes a Windows-like interface that lets users choose from a list of target Web sites provided via the Al-jinan site, select an attack speed (weak, medium, or strong), and the click on the "attack" button.

The concept of "electronic jihad" is a relatively recent strain of cyberterrorism interested in very specific network and economic disruption, [Dorothy Denning](#), a professor in the Department of Defense Analysis at the Naval Postgraduate School, told *InformationWeek*. Its audience consists of malicious Islamic hackers aligned with Osama bin Laden, al-Qaida, and the extremist Islamic movement. "The attacks from jihadists are interested in taking Web sites down and disrupting economies that they don't like," she added. "It's something to be taken seriously."

U.S. businesses would be greatly impacted by any large-scale cyberattacks against either them or the country's critical infrastructure because most of that infrastructure is run by companies in the private sector. The government and the U.S. business community "are one-in-the-same target," [Andrew Colarik](#), an information security consultant who holds a Ph.D. in information systems security from the University of Auckland, told *InformationWeek*. Even businesses that don't run critical infrastructure elements could be affected because "there's a cascading effect if you attack the infrastructure."

Source: <http://www.informationweek.com>



# Cyber Jihad – Cyber Firesale

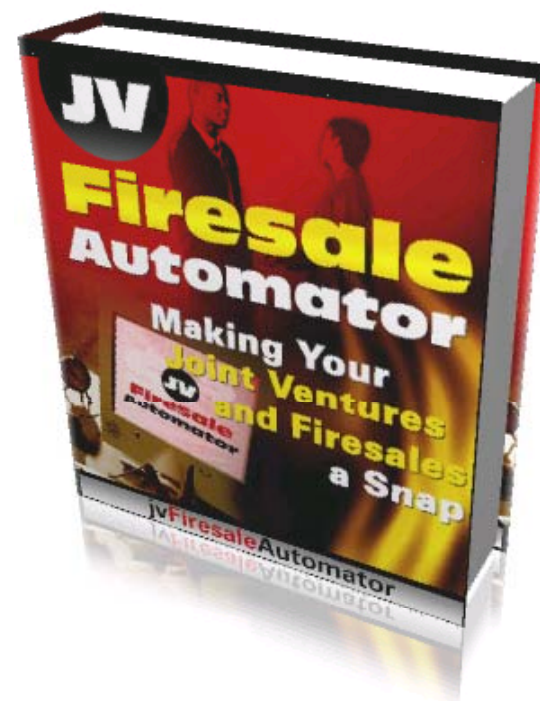
## Cyber Jihad - Cyber Firesale

Submitted by **Jeff Bardin** on Thu, 2007-07-12 15:33. Topic(s): | **Client** | **Corporate Management** | **Data Center** | **Information Security** | **Infrastructure** | **Management** | **Mobile** | **Network** | **Operating Systems** | **Organization Management** | **Personal Management** | **Physical** | **Server** | **Surveillance**

Taking a stroll down memory lane reaching back into my roots, I find a need to discuss the subject of Cyber Jihad or Firesale ( [www.cyberfiresale.com](http://www.cyberfiresale.com) ). Triggered by the recent viewing of 'Live Free or Die Hard' and the concept of an internet or cyber firesale, I find that this blog is an outlet for a subject that gnaws at me on a regular basis.

The combination of a physical and cyber attack using our own infrastructure is inevitable. Attempts have already been made and continue to be made.

It is easy to appreciate the devastation of a physical attack and what it can bring because as Americans, we need to see things in order to understand them. But we must not underestimate the potentially devastating consequences of an electronic attack, especially when used in conjunction with or as a precursor to a physical attack. It may be just that cyber attack that enables the physical attack. Just like our combined sea, air and land battle plans, 'cyber' is a core component.



Source: <http://blogs.csoonline.com/>

Asymmetric Warfare: It's not just for the other guys - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Reload Home Search Favorites RSS Print Mail New Tab Close

Address <http://internet-haganah.com/haganah/> Go Links

---

**הגנה | internet**  
**באינטרנט | haganah**

---

[Home](#) | [Internet](#) | [OSINT](#) | [Off-Topic](#)

---

**13 January 2008**

**New Entries**

**Internet**

- [Al-Qa`ida of Yemen releases their first magazine issue](#)
- [Ah, the old put-a-camera-in-every-room-of-the terrorists'-apartment trick...](#)
- [Avoiding or dealing with arrest - notes based on the experience of the brothers in Iraq](#)
- [Paranoid Drivel of the Week Award goes to...](#)

**OSINT**

- [Former Officers of a Muslim Charity, Care International, Inc., Convicted](#) [13 Jan 2008]
- [Damn those wacky Muslim Boyz](#) [ 9 Jan 2008]
- ["Terror Suspects Hone Anti-Detection Skills"](#) [ 5 Jan 2008]

**Off-Topic**

- [Hot times in the religious schools of Qom...](#)
- [Elements in the US military and intelligence community find the Kool-Aid\\* less-than-palatable...](#)
- [Bush's gift to Israel...](#)
- [Speaking of double standards](#)
- [The Bush Visit and Tensions in the U.S.-Israel Relationship](#)
- [Spitting in the wind is now a matter of policy...](#)
- [Secretary of Defense Robert Gates - the next person to lose his job?](#)
- [An Erev Shabbat message to the Egyptian Foreign Minister](#)

**Contact:**  
contact at sofir dot org

**Support Internet Haganah and the Society for Internet Research**

You can contribute via PayPal:

[Make A Donation](#)

**Mailing list:**  
[Subscribe](#)

**RSS feeds:**  
[Internet](#) | [OSINT](#)

**Search:**  
[Internet](#) | [OSINT](#)

Source: <http://internet-haganah.com/>

Internet Haganah is a project of...

**Society For**



# Mujahedeen Secrets Encryption Program

Mujahideen Secrets 2 is a new version of an encryption tool, ostensibly written to help Al Qaeda members encrypt secrets as they communicate on the Internet


The first edition file contained several encryption algorithms (including AES 256), 2048-bit encryption keys, ROM compression encryption and encryption auto-detection, and file shredding capabilities








The second edition contains automatic message/messaging encryption/authentication and file encryption as well as code signing and checking, and file shredding

This toolset provides groups like Al-Qaida to securely transmit and wipe their files

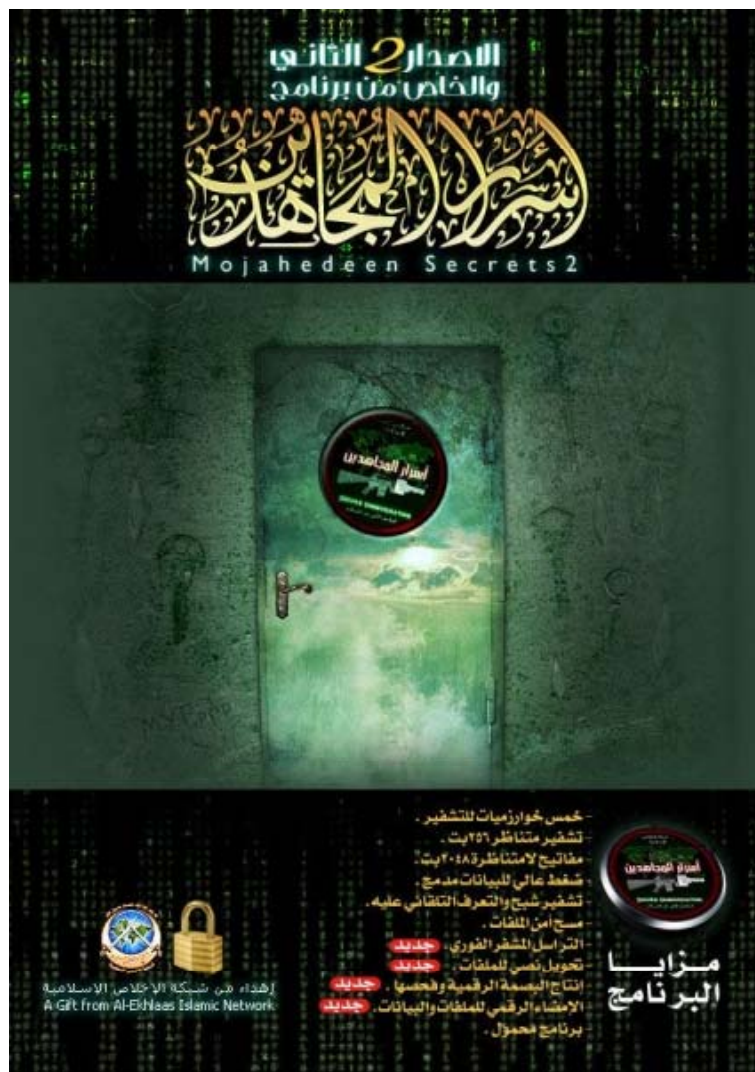
Second edition toolset demonstrates a software development lifecycle with some level of sophistication and planning

# Mujahedeen Secrets Encryption Program: Screenshot 1

Name	Date modified	Type	Size
 new_asr_v2	2/2/2008 4:58 PM	WinZip File	3,151 KB

Name	Date modified	Type	Size	Ta
 Public_Ekhlaas_TSG.akf	1/4/2008 1:39 PM	AKF File	1 KB	
 Asrar_2	1/10/2008 11:50 AM	Application	5,828 KB	
 Asrar.chw	2/2/2008 5:07 PM	CHW File	16 KB	
 Asrar	1/12/2008 5:00 PM	Compiled HTML Help file	2,247 KB	
 AsrarKeys	1/4/2008 3:41 PM	Data Base File	1 KB	
 cover	1/2/2008 10:58 AM	JPEG Image	175 KB	
 Asrar_2.exe.sig	1/10/2008 11:52 AM	SIG File	1 KB	

# Mujahedeen Secrets Encryption Program: Screenshot 2



# Mujahedeen Secrets Encryption Program: Screenshot 3





Cyber terrorism is the use of computing resources against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives

Cyber terrorism can weaken country's economy, by doing this it can strip the country of its resources and make it more vulnerable to military attack

Groups including al-Qaeda use cyberspace for communications, recruiting, and propaganda

Electronic Jihad software is used to let the owner of a computer give control of his system to creator of e-Jihad

Electronic Jihad Program is a part of long-term vision for which jihadi Web site Al-jinan.org has to use the Internet as a weapon

© 1997 Randy Glasbergen. [www.glasbergen.com](http://www.glasbergen.com)



***“I don’t understand #11...  
Thou shalt not be obscene  
on the Internet.”***

Copyright 2000 by Randy Glasbergen.  
[www.glasbergen.com](http://www.glasbergen.com)



"OUR COMPETITION LAUNCHED THEIR WEB SITE, STOLE ALL  
OF OUR CUSTOMERS AND PUT US OUT OF BUSINESS  
WHILE YOU WERE IN THE JOHN."