

Open Intelligence Sources for ITSEC Professionals

By Ronald L. Mendell, MS

The term “intelligence gathering” conjures spies meeting in clandestine alleys passing stolen plans. Actually, intelligence gathering (IG) is a vital activity for ITSEC professionals. Rather than dodging bullets as in the film, *The Bourne Identity*, twenty-first century ITSEC people usually skip the James Bond theatrics. But, they still must see the world through different eyes than their client or employer.

What then are the goals of IG for the ITSEC professional? **First**, exploring perimeter defenses through Google® hacking reveals what portions of the organization’s network face unintended exposure. Using search engine inquiries, what can an adversary learn about the configuration of the network? In spite of the wisdom that firewalls protect all, or the fact that the vulnerability scan found no glaring holes, the ITSEC professional still seeks an adversary’s perspective. By carefully crafting search engine inquiries, the network’s hidden, yet still Web-facing, elements rise into the realm of visibility.

Second, gathering intelligence about the client organization through the Internet or media sources uncovers information leakage. Such leakage is often unintended. But the lack of malice in its dissemination makes the data no less severe in its impact. Sensitive data gets into a news group posting, into a publication, or remains on a document that unintentionally faces the Web. Systematic online inquiries about the organization and its intellectual property, whether through a variation of Google hacking or by other research means, often locates and stymies leaks early in the process, which minimizes the damage.

Learning about Internet-based threats is the **third** reason for IG. These threats include the latest malicious code, OS vulnerabilities, and new exploits. Internet scams that victimize the organization’s customers, vendors, and suppliers also warrant intelligence gathering and analysis.

Fourth, reconnaissance of the organization’s Web site often tells an interesting story. A form of intelligence gathering closest to home, the “story” reveals guideposts and clues available to a would-be attacker. From data available on the Web site, an intruder may be able to impersonate members of the IT staff, to mimic internal e-mail addresses, or to learn about defenses in place. Knowing about publicly available information concerning the client organization can assist in making sure that the Web site is not too helpful to hostile visitors.

Finally, IG allows the collection of actionable information about extremist and terrorist activities. Obviously, key focal points are New York, Washington, D.C., and London. A client having operations in these cities needs an effective IG effort. Be aware, however, extremist or terrorist activity can present itself anywhere a suitable target exists. Threats and targets do change. Evaluating the client’s security posture in the light of changes in the social, political and economic climate is a part of the security professional’s job. And IG can help that effort.

Google Hacking

The term “Google hacking” is a double misnomer that serves as a handy word of art for this discussion. Actually, search engines other than Google can assist in searches similar to the ones identified here. And, whether by entering the Google “hack” manually or by using a Web robot or a Google API, no illegal intrusion into a system occurs. Instead, the search methodologies simply uncover documents on Web pages and system configuration information not intended by the owner.

Web-facing documents or information, where sensitive data may pass on to savvy hunters, is the bane of the security investigator’s lot. In defense of the client’s realm, the

ITSEC professional does some searches of his or her own. An example of a fundamental search is: “exploits site:microsoft.com.” Yielding all pages containing the word “exploits” on the designated site, this search looks for key, sensitive terms. (A listing of other general search terms is in Figure 1.) Searching by specific product names, projects, technical processes, and by other internal terminology is also feasible. For example, the search term, “‘process alpha’ site:<client site>” ensures “process alpha” is not mentioned in Web-facing documents.

In addition to textual searches by selected terms, Google “hacks” also examine a page’s title, its URL, a page’s file type, and its links to other pages. For example, to see all Web pages containing “login” in the title and “password” in the body of the page, use the search: “intitle: login password site:<client’s site>.” And, the search phrase “inurl: passwd site: <client’s site>” identifies any unintended guideposts to passwords.

Beyond uncovering information leakage, Google hacking also does additional duty by pointing the finger at directory and configuration vulnerabilities. (See Figure 2.) Index browsing of Web servers becomes easy with phrases like: “Index of /admin”, “Index of /cgi-bin”, or “inurl:config.txt.” Vulnerable sites yield clues to security holes through searches similar to: “inurl:admin filetype:txt”, “inurl:webeditor.php”, and “inurl:file_upload.php.” Access to data in any of these files may permit the compromise of a system or server. Combining syntaxes for increased granularity results in these searches: “intitle: ‘Index of ’ .sh_history” or “intitle: ‘Index of ’ master.passwd.” And, adding the parameter “site:<client’s site>” is possible to any of these searches. A strong resemblance exists between anti-virus and IDS signatures and the search phrases used to detect vulnerabilities via Google hacks. Knowing the vulnerability’s key phrases or the specific text patterns that it looks for

Sensitive Hit List:
"Customer list"
"Marketing plans"
"Quarterly financials"
"Year-end financials"
Acquisition
Admin
Administrator
Classified
Confidential
Exploit or Exploits
Internal
Login
Merger
Password
Restricted
Secret
Sensitive

Figure 1: General Word List for Google Hacking

makes the crafting of Google hacks quite straightforward.

Information Leakage

Other intelligence sources, besides Google hacking, to detect information leakage are available through the Internet. A fundamental shortcoming in any security strategy assumes technical security alone protects a client's assets. Humans are fallible; information leakage is a common byproduct of them doing business. Yet wisely using intelligence-gathering resources allows the uncovering of leaks.

Four major sources offer intelligence tools: the "Internet Stream," commercial feeds, gray sources, and human experts. The Internet Stream includes data derived from Google hacking, RSS (Real Simple Syndication) feeds, Google News, Google Groups, Yahoo!® Alerts, Dialog NewsEdge, Blogs, and Nexcerpt reports. With an RSS reader on a computer, the ITSEC professional can arrange for any RSS news source to feed updates into the reader. Many information and news sites now provide RSS capability and identify themselves with the red RSS icon on their site. RSS allows the creation of a highly customized news service using tags or topics. (See Figure 3).

Google News is a free service that allows the filtering of multiple news sources based upon a search term. The search term can be the client's corporate or business name. It can be a vulnerability or a threat like "phishing" or a key person's name. Changes are possible in seconds based upon current intelligence needs. Google News is very effective as a quick and easy intelligence filter for Web-based news services and feeds. Yahoo! Alerts will send alerts to a computer, a

Search Phrase	Purpose
exploits site:microsoft.com	Looks for the word "exploits" on this site
allintitle: login password site:Microsoft.com	Locates the words "login" and "password" on the site
allinurl:etc/passwd	Looks for sites that have "etc/passwd" in their URL
filetype:doc site:edu confidential	Locates educational sites that have the word "confidential" in MS Word format. (The site parameter can be a full URL.)
link:www.securityfocus.com	Identifies all other sites linking to this one.
Index of /admin	Searches for browser directories with the "admin" subdirectory. (Site parameter can also be used.)
Index of /mail	Searches for browser directories with the "mail" subdirectory. (Site parameter can also be used.)
inurl: bash_history	Locates sites with the Bash history in their URL.
inurl:mysql filetype:cfg	Looks for configuration files in MySQL URLs. A way to find users.
intitle:"Index of" members or accounts	Looks for a directory of members or accounts in the page title.
allinurl:/scripts/cart32.exe	Sites prone to XSS attacks
allinurl:/privmsg.php	Vulnerability to SQL Injection attacks

Figure 2: Examples of Google Hacking Phrases

Source	Location	Content
Google hacking: 1. Useful for detecting information leakage 2. Can identify OS and configuration vulnerabilities	http://www.google.com	<ul style="list-style-type: none"> Filetype (looking for a specific document or format) Link (other sites that show the targeted site as a link) Inurl (searching the contents of the URL, allinurl searches for multiple terms) Intitle (searching the contents of the page's title) Site (specifying the site to be searched)
RSS (Real Simple Syndication)	"Introduction to RSS" at http://www.webreference.com/authoring/languages/xml/rss/intro/	To locate RSS feeds, use this directory at http://chordata.info/ . Must download a RSS reader.
Google Groups	http://groups-beta.google.com/?hl=en	Access to news groups.
Google News	http://news.google.com/nwshp?hl=en&gl=us	Customizable news feed page on selected topics.
Yahoo! Alerts	http://alerts.yahoo.com/main.php?view=spl&ash_signup_signin&.done=http%3A%2F%2Falerts.yahoo.com%2F	Customizable news alerts on selected topics.
Dialog NewsEdge	http://www.dialog.com/newsedge/	A highly customized report of news relevant to a search interest.
Blogs	A directory of blogs at http://www.blogwise.com/ . A blog is personalized journalism; usually, it represents the focus of an individual or a group on a given topic or area of interest.	An example of an ITSEC blog: http://www.volubis.com/blog/
Nexcerpt	http://www.nexcerpt.com/	An electronic clipping service that selects news and information according to filters designated by the subscriber. An invaluable intelligence gathering tool.

Figure 3: Internet Streams

PDA, or a message-capable cellular telephone based upon filters selected by the user. It can be an on-the-go intelligence tool and watchdog.

Google Groups provides access to news group discussions on virtually every topic under the sun. Discussions in news groups may reveal

hackers talking about the client's network or vulnerabilities. Postings by employees could disclose sensitive information. For example, software developers often post requests for technical assistance from other professionals in the field. While these requests have good intent behind them, such postings could inadvertently reveal sensitive or proprietary information.

Dialog's NewsEdge offers a personalized business news service of good intelligence quality. A wide range of databases and news sources at its disposal, Dialog can deliver a customized news page based upon the user's search filters. Like Nexcerpt described below, NewsEdge is a higher-end intelligence tool for monitoring possible information leakage.

Blogs are a blend of personal journalism, gossip, opinion, and links to areas of interest by the individual or group running the blog. While at times biased and opinionated, blogs can be a source of useful intelligence about an industry, a technology, and social events relevant to a client, and often serve as vectors for information leakage. Even ITSEC blogs exist. Many blogs have internal search engines that aid in their intelligence value. On one recent ITSEC blog, for example, an internal search yielded several references about a records management company experiencing information security problems. So, treat blogs as one way to uncover what sensitive information about a client is passing about cyberspace. And, as an added bonus, some blogs offer RSS feeds, which aid in centralizing the data collection effort.

Another automated intelligence agent is Nexcerpt. This service allows preset searches of data from magazines, newspapers, news Web sites, trade journals, wire services, online portals, news groups, blogs, certain Intranet servers, and subscription databases. Providing customized intelligence reports, Nexcerpt keeps an eye on mentions of a client and of events in the client's industry. A sophisticated tool for mining both the surface and substrata levels of wide range of data streams, Nexcerpt is for serious monitoring of information leakage.

Commercial feeds like Factiva, Dialog, Lexis-Nexis, STN, and Questel-Orbit offer a different dimension to investigating information leakage. They are serious research tools and require more investment of time and money than the Internet Streams. Yet, in complex intellectual property theft cases, they provide greater depth. (See Figure 4.) With over 9,000 sources, Factiva places online news and factual sources within the easy reach of any search term. Lexis-Nexis also holds a vast

Source	Location	Content
Factiva	http://www.factiva.com/	"More than 9,000 sources from 152 countries in 22 languages, including more than 120 continuously updated newswires. And, more than 900 sources are available on or before the date of publication." -from Factiva site
Dialog	http://www.dialog.com/	Access to hundreds of databases in technology and business intelligence.
Lexis-Nexis	http://www.lexisnexis.com/	An excellent source of commercial intelligence for an industry or for a specific company. Offers hundreds of news sources and public records.
STN	http://www.stn-international.de/	A valuable resource if the client operates heavily in the scientific or technical sector. Access to over 220 databases provided by scientific organizations worldwide. Very useful for tracking developments in a given technology.
Questel-Orbit	http://www.questel.orbit.com/index.htm	A gateway to intellectual property (patents and trademarks) databases worldwide. Useful in investigations of intellectual property theft.
Internet Threats		
AT&T Internet Protect™	http://www.business.att.com/emea/internet_protect/	Identifies Internet threats through AT&T's global IP backbone. An alert service by subscription.
SANS	http://isc.sans.org/	Internet Storm Center offers a Web page on current threats.
Internet Security Systems	https://gtoc.iss.net/issEn/delivery/gtoc/index.jsp	ISS offers a dashboard on threat levels and the X-Force™ Threat Analysis Service by subscription.

Figure 4: Commercial Feeds

store of news feeds and resources for researching almost any topic. STN specializes in scientific and technical resources. Questel-Orbit offers access to intellectual property databases for patents and trademarks.

As with any intelligence gathering system, a budget plan is essential. Sharing resources with another department often yields cost savings. For example, when the organization has a business intelligence unit (BIU), teaming up on commercial feeds may save money. In setting intelligence objectives and a budget for IG, keep in mind three factors: coverage, goals and ease of use.

Coverage means the depth and extent of the IG effort. The needs of the organization govern coverage. A comprehensive IG plan to assess a client's information security posture blends Internet threat surveillance, the detection of information leakage, and the gathering of industry or competitive intelligence. As far as ease of use goes, the focus becomes on either obtaining alerts or on doing in-depth research.

For detecting information leakage on a low budget, the following resources tend to be alert-oriented or involve quick scanning for key facts:

- ▲ RSS feeds
- ▲ Yahoo! Alerts
- ▲ Google News

Medium-level research sources, which require moderate expenditure of time, are:

- ▲ Google Groups
- ▲ Dialog NewsEdge
- ▲ Nexcerpt
- ▲ Researching Blogs

Intensive research sources for information leakage and intellectual property theft investigations are:

- ▲ Factiva
- ▲ Dialog
- ▲ Lexis-Nexis

- ▲ STN
- ▲ Questel-Orbit
- ▲ Google hacking

Alerts from “free” sources are appropriate for any ITSEC intelligence program. They consume minimal research time and provide quick snapshots of what is happening in the client’s industry. In addition, they key in on where and when the client’s name appears on the Web. They act as a distant early warning system.

Medium-level research sources allow investigations into the rumors, the near truths, and the sensitive information being passed on news groups by friendly parties and by hostiles. Blogs offer similar intelligence value regarding informal information passing across cyberspace concerning the client. Services like Nexcerpt and Dialog NewsEdge yield news digests about the client and the client’s industry in a compact format. When information leakage becomes a mid-range threat, these resources offer deeper view at reasonable cost.

Intensive research sources address serious compromises of sensitive information and intellectual property. Knowing about patents, scientific developments, changes in technology, and new product releases all figure into an investigation. Google hacking takes time too in probing all the various phrases that may indicate compromise. Yet it may be a productive endeavor on a periodic basis for almost any organization. With search engine probes, an ITSEC professional may locate holes in the dike before a leak becomes a flood.

Intelligence About Internet Threats

AT&T Internet Protect™ is an alert service based on incidents arising from AT&T’s Internet backbone. It provides intelligence on Internet threats worldwide such as exploits, denial of service, and malicious code attacks. Subscribing to this service offers a formal method for IG regarding cyberspace. (See Figure 4.)

SANS Internet Storm Center is a Web-based clearinghouse on warnings and alerts pertaining to the Internet. It provides a free window on what could be coming the client’s way regarding possible network attacks. Internet Security Systems has a free Web-based dashboard on Internet threat levels coupled with alerts on major threats. For more in-depth coverage, ISS has X-Force™ Threat Analysis Service available by subscription.

Google News or any of the Internet news feeds previously mentioned can provide free or

Categories	Specific Sources
Private security reports and publications	<ul style="list-style-type: none"> • American Society for Industrial Security (ASIS): <i>SecurityManagement Daily</i>, available as an e-mail newsletter to ASIS members on general and IT security threats • ISSA Chapters’ Web sites • <i>SecurityManagement Online</i> at http://www.securitymanagement.com/ • SecurityFocus at http://www.securityfocus.com/ • Whitepapers (try “filetype:pdf security whitepapers” on Google)
Conferences	<ul style="list-style-type: none"> • ASIS • ISSA National and Local • HTCIA (High Technology Crime Investigation Association)
Informal networking	<ul style="list-style-type: none"> • Local law enforcement high-tech unit • Local ASIS/ISSA chapter • Regional security meetings
Contacts Online	<ul style="list-style-type: none"> • Reporting Internet Crime at http://www.cybercrime.gov/reporting.htm • Critical Information Protection Resources at http://www.dhs.gov/dhspublic/display?theme=74 • InfraGard at http://www.infragard.net/
Homeland Security feeds	DHS’s Homeland Security Information Network, Critical Infrastructure (HSIN-CI) daily updates on domestic security and international security events via e-mails. Contact https://www.swern.gov/forms/enrollrequirements.php for more details.
Human Experts	<ul style="list-style-type: none"> • STN • Dialog • Factiva/Lexis-Nexis • <i>Encyclopedia of Associations</i> at http://www.infoplease.com/ipa/A0004878.html (abridged version online) • Resources listed above in other categories

Figure 5: Gray Sources and Human Experts

low-cost coverage of Internet-related threats. (See Figure 3.) Setting appropriate filters like “Internet Malicious Code,” “Internet Denial of Service,” “Internet Scams,” “Internet Phishing,” and so on should capture useful intelligence to supplement any paid sources.

Gray sources are either based upon informal networking among members of the security community or transmit news not geared to the general public, usually specialized security publications. (See Figure 5.) In addition to specialized online and print publications like *Security Management* magazine and SecurityFocus, conferences, local chapters of security organizations, online contacts, and Department of Homeland Security e-mail feeds constitute reliable gray source intelligence. Human experts (as opposed to databases as a source of expertise) are another gray source. Experts may be necessary in tracing information leaks in an organization, in providing computer forensics expertise, in analyzing crime or terrorist trends in a given

region or those affecting a certain industry, or in providing technical expertise regarding specific attacks on the client’s network. Sources for locating experts include STN, Dialog, Factiva and Lexis/Nexis, and the *Encyclopedia of Associations*, whether online, or in the print version found in most libraries. Of course, the previously mentioned gray sources can yield leads for locating experts.

In addition, CERT (<http://www.cert.org>), SecurityFocus, and AT&T’s planned online channel for twenty-four hour news about Internet security all offer direct updates on specific threats. If a client maintains a Network Operations Center (NOC), as many of these resources as is feasible should be available to the NOC staff and to on-duty information security personnel.

Site Reconnaissance

When an ITSEC professional does a site reconnaissance, he or she is not doing pene-

tration testing or vulnerability analysis via scanning through a tool such as Nmap. Instead, the focus is on gaining intelligence on the client much like an adversary would do in the earliest stages of planning an intrusion. The first step in reconnaissance is to learn as much from public sources as possible about the client. A fundamental rule of thumb is business information has far fewer restrictions on its dissemination than data about individuals. A potential wealth of information then resides in the public sector about most companies and organizations.

Key factors to learn about a business are: (1.) Its organizational structure, including its principal operating officers, (2.) Contact information such as e-mail addresses and telephone numbers for various departments, (3.) Biographical information about its officers and key IT staff, (4.) Business locations including data processing centers, (5.) The contents of its Web sites, and (6.) Any information about its IP addresses and servers. With this preliminary business background data, a hacker develops footholds with which to attack the client.

The resources identified in Figure 6 supplement intelligence from news feeds and commercial sources listed in Figures 3 and 4. Most of the business Web sites provide company profiles and access to public records such as corporate filings about the client. Again, knowing as much as the client and the client's industry is an effective way to identify possible avenues of attack. Learning biographical information about the IT director, for example, aids in social engineering attacks and even impersonation of this individual.

While public information is nearly impossible to eliminate or to lock down, its impact can be minimized through IG efforts. An ITSEC professional can make sure that passwords and usernames are not derivative from a key IT staff member's publicly available biography. Training staff in verification procedures based on information not publicly disseminated reduces social engineering and impersonation attempts. But first, the ITSEC person has to know what is out there, and IG efforts can do that.

In addition, eyeballing IP registration information and scanning the client's Web sites for content that may be too revealing, offering too many guideposts, is a sound preventive control. If the site says John Q. Jones is the Director of Information Systems at 512-555-6666, and his e-mail address is jjones@clientcompany.com, consider supplying a general telephone number and e-mail address for the department and not divulge who the director is. Again, if the ITSEC staff is not

Category	Locations	Information
Business Web Sites	<ul style="list-style-type: none"> Hoovers http://www.hoovers.com/ Yahoo Finance http://finance.yahoo.com/ Edgar http://www.sec.gov/edgar.shtml Patents and Trademarks http://www.uspto.gov/ Secretary of State Texas (Corporate Records) http://www.sos.state.tx.us/corp/sosda/index.shtml (for other states' corporate records) http://www.nass.org/busreg/corp/eg.html Choicepoint https://www.choicepointonline.com/default.asp USSearch http://www.ussearch.com/business/webflow?cid=1603&action=browsecategory 	Publicly traded companies have the most free data online. Choicepoint and US Search are fee-based services.
Whois	<ul style="list-style-type: none"> Sam Spade http://www.samspade.org/ ARIN http://www.arin.net/whois/index.html 	Sam Spade offers access to most Whois engines.
Web Site Scanners	<ul style="list-style-type: none"> BlackWidow http://www.softbytelabs.com/Frames.html DominoScan http://www.nextgenss.com/dominio.htm 	These tools scan and capture the entire site. They focus on site content.
What the Site Reveals about the Organization	<ul style="list-style-type: none"> Names of Officers and IT staff Key telephone numbers and locations 	Also e-mail addresses, even IP addresses, organizational charts, directories.

Figure 6: Client Site Reconnaissance

"nosy" about what is easily available via the Web, then preventive steps cannot be done.

Monitoring Terrorism and Extremists

The average ITSEC professional does not have to be an expert on terrorism or domestic extremist activity. A contract with CNN, CBS, ABC, or NBC as a terrorism expert is not a requirement for most ITSEC jobs. Short of being a scholar on the subject, however, an ITSEC professional should be familiar with some common intelligence sources in this area. The sources cited in Figure 7 will help.

A leap from the realm of familiarity to constant, active intelligence collection could arise from a change in the client's business activity. Acquisition of a division that does SCADA technology (control of critical infrastructure systems such as power generation and distribution) would be an exam-


ple. Locating operations in a country with heightened terrorism activity is another example. (The "hot spots" are not all in the Middle East. Reviewing chronologies of international terrorism reveal India, the touted locale for high-tech outsourcing, has a large number of terrorist incidents. Latin America has its share, too. And of course, there are the recent events in Europe.)

If the client becomes involved in research or operational activities that offend domestic extremist groups, be aware that attacks on the client's networks and Web sites are a real possibility. Physical attacks against insecure data facilities are another possibility. For example, animal rights extremists have attacked various medical research facilities in the U.S.

When serious IG efforts become necessary in this area, an ISEC professional can find that subscribing to services such as Jane's Terrorism and Security Monitor to be very much in order. In addition, virtually every resource mentioned in

this article can come into play to develop in-depth private source intelligence on Terrorism. Often, numerous news feeds play essential monitoring roles. Also, gray sources become very useful in this arena. Specific terrorism threats may require engaging human experts to address particular concerns. For example, if a client had an IT operation in London in the summer of 2005, that IT team may need specific guidance on conducting operations in light of the increased terrorist activity in Britain.

Putting It Together

Gathering intelligence from private sources in a nutshell involves tapping into news sources, knowing how to conduct Web search engine inquiries, locating gray sources, and being able to do research on commercial databases. The amount of time and money invested in IG depends upon the probable threats the client faces. Analysis of the data requires two fundamental yardsticks. First, a source has to be evaluated on its reliability. What is its track record on being correct? If a service or database has a reputation for carefully screening and verifying information before disseminating the data, it probably can be relied upon in a critical situation. And second, the other issue is validity. How does the source correspond to reality? Can the source be verified by other sources? Relying on gossip in a blog or on a news group may not be a sound practice in a crisis unless other reliable sources confirm the information. Always strive to use these two yardsticks in analyzing information from intelligence sources. 

Ronald Mendell works for a high-tech company in Austin. He holds a Master of Science degree in network security and is a freelance writer specializing in investigative and security topics.

Source or Topic	Location	Content
CIA World Factbook	http://www.cia.gov/cia/publications/factbook/	Free online guide to the countries of the world
Terrorism Research Center	http://www.terrorism.com/index.php	A mix of free and paid-by-subscription documents and alerts
Jane's Terrorism and Security Monitor	http://jtsm.janes.com/	Paid-by-subscription updates on international terrorist developments
National Terror Alert Resource and Information Center	http://www.nationalterroralert.com/	Private site that posts access to free articles on terrorist activity.
Domestic Terrorists and Extremists	Search engine inquiries under "ecoterrorists," "animal rights extremists," "American militias," "Neo-Nazi groups," "racist or hate organizations," or under a specific group's name.	If the client is in an industry targeted by any domestic extremist group, Web searches can produce useful intelligence on the group's leadership, ties, organization, tactics, and even funding.
Cyberterrorism	"The Truth About Cyberterrorism" (<i>CIO Magazine</i> , March 15, 2002) http://www.cio.com/archive/031502/truth.html "The Spectrum of Cybermalfeasance" http://www.cio.com/archive/031502/truth_sidebar1.html Technical Support Working Group Site on SCADA http://www.tswg.gov/tswg/ip/scada.htm	An area of concern populated by "buzz" words. Protecting data may be the paramount concern. SCADA protection is another vital area.
Chronologies	"Hacker Timelines" http://en.wikipedia.org/wiki/Timeline_of_hacker_history http://www.xtvworld.com/news/hackerframe.htm Chronology of International Terrorism for 2004 http://www.tkb.org/documents/Downloads/NCTC_Report.pdf	Timelines offer perspective; for example, India, a hotbed of technology, is also one for terrorism.

Figure 7: Terrorism and Extremist Activity

Resources

- ▲ "Google Hacking 101," edited by Matt Payne, CISSP, June 15, 2005.
<http://www.necert.org/CSF/CSF-Jan2005.pdf>
- ▲ "The Google Hacker's Guide," by Johnny Long, (no date).
http://johnny.ihackstuff.com/security/premium/The_Google_Hackers_Guide_v1.0.pdf
- ▲ *Google Hacking for Penetration Testers*, by Johnny Long, Syngress, 2004. "Demystifying Google Hacks," by Debasis Mohanty, (no date).
http://www.infosecwriters.com/text_resources/doc/Demystifying_Google_Hacks.doc
- ▲ *NATO Open Source Handbook*
http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf