Cyber Terrorism: A Study of the Extent of Coverage in Computer Security Textbooks

Janet J. Prichard and Laurie E. MacDonald
Bryant University, Smithfield, RI, USA

prichard@bryant.edu lemac@bryant.edu

Executive Summary

On September 11th, 2001 the United States experienced the largest terrorist attack in its history. This event caused many government agencies to review their security practices and procedures. It also has raised awareness of other avenues that terrorists might pursue to achieve their goals, including cyber terrorism. Cyber terrorism can be described as politically motivated attacks in cyberspace. These attacks are intended to cause grave harm, such as loss of life or severe economic damage. Often the term "weapons of mass disruption" is used in describing these potential computer-based threats.

The threat of these attacks intensified the need for more computer professionals to have computer security expertise. It also pointed to the need for students studying computer related fields to be exposed to topics in computer security, particularly the threat posed by cyber terrorism.

We examined a random sample of sixteen textbooks in the field of computer security to determine the coverage dedicated to cyber terrorism. Textbooks typically provide resources for faculty to teach students various topics in a course – in this case resources to help students understand the potential threats, techniques, and targets of cyber terrorists.

The results show that computer security textbooks do not give cyber terrorism the depth of coverage warranted by its significance for the IT industry. Therefore, faculty need to find their own references and re-sources to address cyber terrorism adequately in their class. This paper concludes by providing numerous web sites and trade books that can be used to help faculty provide more information to their students on cyber terrorism.

Keywords: Cyber terrorism, computer security, information warfare, infrastructure targets.

Introduction

Terrorism is the most pressing national security issue facing the United States and its allies around the world. This became shockingly clear on September 11, 2001 and promises to be a long-lasting threat requiring a total commitment by the United States to eliminate terrorist organizations wherever they are found. Terrorism is an old problem, and the word terrorism dates to France's Reign of Terror in 1793-94 (Garrison, 2003). The United States State Department has defined terrorism as violence against noncombatants for the purpose of influencing public opinion (Council on Foreign Relations [CFR], n.d.).

Editor: Lynn Hunt

The former deputy chief of the CIA Counterterrorist Center has identified four elements that are common to all acts of terrorism (Vatis, 2001). Acts of terrorism are: (1) premeditated and not simply acts born of rage, (2) political and designed to impact political structure, (3) targeted at civilians and civilian installations, and (4) conducted by ad hoc groups as opposed to national armies. The war on terrorism is sure to result in cyber attacks against US assets launched by terrorist groups, nation-states that provide support for terrorists, and hackers who sympathize with the terrorists (Vatis, 2001).

The term "cyber terrorism" was coined to characterize computer-based attacks against an adversary's assets. It takes place were cyberspace and terrorism converge (Denning, 1999). Though these attacks occur in cyberspace, they still exhibit the four elements common to all acts of terrorism:

(1) premeditated and not simply acts born of rage

Cyber terrorist attacks are premediatated and must be planned since they involve the development or acquistition of software to carry out an attack.

(2) political and designed to impact political structure

Computer terrorism is an act that is intended to corrupt or completely destroy a computer system (Galley, 1996). Cyber terrorists are hackers with a political motivation, their attacks can impact political structure through this corruption and destruction.

(3) targeted at civilians and civilian installations

Cyber terrorist attacks often target civilian interests. Denning (2000a) qualifies cyber terrorism as an attack that results in violence against persons or property, or at least causes enough harm to generate fear.

(4) conducted by ad hoc groups as opposed to national armies

Cyber terrorism is sometimes distinguished from cyber warfare or information warfare, which are computer-based attacks orchestrated by agents of a nation-state.

Cyber warfare is another term that is often used to describe various aspects of defending and attacking information and computer networks in cyberspace, as well as denying an adversary's ability to do the same (Hildrith, 2001). Cyber warfare and information warfare employ information technology as an instrument of war to attack an adversary's critical computer systems (Hirsch, Kett, & Trefil, 2002). Winn Schwartau (1994) has proposed three categories for classifying information warfare: (1) Personal Information Warfare, (2) Corporate Information Warfare, and (3) Global Information Warfare.

Personal Information Warfare involves computer-based attacks on data about individuals. It may involve such things as disclosing or corrupting confidential personal information, such as those in medical or credit files. Corporate Information Warfare may involve industrial espionage or disseminating misinformation about competitors over the internet. Global Information Warfare is aimed at a country's critical computer systems. The goal is to disrupt the country by disabling systems, such as energy, communication or transportation.

Another level of politically motivated computer attacks is often referred to as hacktivism – a combination of political activism and hacking. The intent in hacktivism is to disrupt normal operations but not cause serious damage (Denning, 2000b). These may include web sit-ins, automated email floods, and weak viruses. Hence, hacktivism is distinguished from cyber terrorism by the level of damage and disruption intended by the politically motivated hackers.

Hacking Techniques – Types of Attacks

Galley (1996) discusses three types of attacks against computer systems: (1) Physical, (2) Syntactic, and (3) Semantic. A physical attack uses conventional weapons, such as bombs or fire. A syntactic attack uses virus-type software to disrupt or damage a computer system or network. A semantic attack is a more subtle approach. Its goal is to attack users' confidence by causing a computer system to produce errors and unpredictable results.

Syntactic attacks are sometimes grouped under the term "malicious software" or "malware". These attacks may include viruses, worms, and Trojan horses. One common vehicle of delivery for malware is email.

Syntactic attacks also include denial of service (DOS) and distributed denial of service (DDOS) attacks. These types of attacks have become more widespread in recent years. One common form of DOS and DDOS attacks use a technique known as ping saturation (Vatis, 2001). Ping is a simple Internet utility used to verify that a device is available at a given Internet address. Ping saturation occurs when ping is used in an attack to overwhelm a system. The intent in these types of attacks is to disrupt services on a network or system by flooding it with requests.

Semantic attacks involve the modification of information or dissemination of incorrect information (Schneier, 2000). Modification of information has been perpetrated even without the aid of computers, but computers and networks have provided new opportunities to achieve this. Also, the dissemination of incorrect information to large numbers of people quickly is facilitated by such mechanisms as email, message boards, and websites.

Examples of Computer-Based Attacks

India and Pakistan have engaged in a long-term dispute over Kashmir. The dispute moved into cyberspace when pro-Pakistan hackers began repeatedly attacking computers in India. The number of attacks has grown yearly: 45 in 1999, 133 in 2000, 275 by the end of August 2001 (Vatis, 2002). At least one of these groups, the Pakistan Hackers Club, has also attacked American assets, namely, web sites maintained by the US Department of Energy and the US Air Force.

The Israel-Palestine conflict saw its first cyber attacks in October 2000 when some Israeli teenagers launched DOS attacks against computers maintained by the Palestinian terrorist organizations Hezbollah and Hamas (Kraft, 2000). Anti-Israel hackers responded almost immediately and crashed several Israeli web sites by flooding them with bogus traffic. Among the Israeli sites attacked by the Palestinians were sites belonging to the Knesset (parliament), Israeli Defense Forces, the Foreign Ministry, and the Bank of Israel.

When planes from the North Atlantic Treaty Organization (NATO) bombed targets in Kosovo, the NATO computers suffered sustained attacks (Nuttall, 1999). Approximately 100 web servers run by NATO were subjected to ping saturation. At the same time numerous American military and commercial web sites were defaced by Russian, Chinese, and Serbian hackers. These attacks did not affect the command and control systems for the NATO bombing but did impact NATO's efforts to use the Internet to launch a propaganda campaign to gain support for ending the regime of Milosovic. One of the NATO web sites attacked carried messages from NATO detailing the atrocities of Milosovic and justifying the bombing.

The mid-air collision of an American surveillance plane and a Chinese fighter aircraft in 2001 engendered a political and diplomatic dispute between the two countries. The political conflict was accompanied by an online campaign of cyber attacks carried out by both sides, with hackers around the globe joining in (McWethy & Starr, 2001; Vatis, 2002). The Honker Union of China and the Chinese Red Guest Network Security Technology Alliance organized a vigorous campaign of cyber attacks against American targets. Approximately 1,200 US web sites experienced

DOS attacks and/or defacement. It is an open question as to whether the Chinese government sanctioned these attacks. An American hacker group called PoizonBox claimed it had defaced more than 100 Chinese web sites.

Research Statement

This research argues that cyber terrorism is a critical issue for the computer industry and society in general. Therefore, it is very important that IT faculty develop ways to teach our students how to identify and prevent cyber terrorism in the future.

Methodology - Text Analysis

Table 1 lists the collection of Computer Security texts assembled for review and evaluation. The methodology used to select the textbooks was similar to that used to search for a textbook for actual course use. An effort was made to select the most recently published editions given the new emphasis on security after September 11th, 2001. The researchers started with a list of academic publishers they commonly use in searching for IT textbooks. This list was expanded by adding entries found by searching Yahoo's list of academic publishers. Each of the publishers' sites was searched to determine if they marketed a textbook targeted for use in an undergraduate course on computer and information security. Requests for approximately twenty textbooks were made to ten publishers. The researchers obtained sixteen security related textbooks from this effort and used these to conduct the study.

Table 1: Textbooks examined in this study

Bishop, Matt. (2003), Computer security: art and science. Addison-Wesley / Pearson Education.
Bosworth, Seymour, & Kabay, M. E. (2002). Computer security handbook, 4th Edition. Wiley.
Campbell, Paul & Boswell, Steven. (2003). Security+ in depth. Course Technology.
Dalton, Dennis. (2003). Rethinking corporate security in the post 9-11 era. Morgan Kaufmann.
Day, Kevin. (2003). Inside the security mind: making the tough decisions. Prentice Hall.
Jamska, Kris. (2002). Hacker proof (2nd ed.). Thomson / Delmar Learning.
Kovacich, Gerald. (2003). Information systems security. Butterworth Heinemann / Elsevier.
Liska, Allan. (2003). The practice of network security: Deployment strategies for production environments. Prentice Hall PTR.
Mackey, David. (2003). Web security for network and system administrators. Course Technology.
Maximum security. (2001). Sams Publishing.
McCarthy, Linda. (2003). IT security, risking the corporation. Prentice Hall PTR/ Pearson Education.
Panko, Raymond. (2004). Corporate computer and network security. Prentice Hall.
Pfleeger, Charles P. & Pfleeger, Shari Lawrence. (2004). Security in computing, 3/E. Prentice Hall PTR.
Pipkin, Donald L. (2003). Halting the hacker: A practical guide to computer security (2nd ed.). Prentice Hall PTR.
Rittinghouse, John W. & Hancock, Bill. (2003). Cybersecurity operations handbook. Digital Press / Elsevier.
Tjaden, Brett. (2004). Fundamentals of secure computer systems. Franklin, Beedle and Associates.

A content analysis of the texts was undertaken by the researchers to determine the extent of coverage provided by these textbooks. Three Computer Information Systems professors and one graduate student pursuing a Master of Science degree in Information Systems carried out this textbook analysis independently. Each researcher gathered data on each text and the results were averaged. For example, each researcher may have determined different counts for the number of pages for a particular category. This was due to the fact that they interpreted the information contained in the texts in a slightly different manner. Their results were then averaged together to yield an approximate page count for that category.

The content evaluation was based on methodologies used in similar textbook studies including: (1) the model developed by the American Association for the Advancement of Science. (Kulm, Roseman, & Treistman, 1999), (2) the technique employed by Leif (1994), and (3) the technique employed by MacDonald and Fougere (2003).

Originally, three major categories of terms related to cyber terrorism were selected to focus the analysis. These categories were based upon the intentions of the attacks (Intent), the targets of the attacks (Targets), and the techniques used to produce the attacks (Techniques). If one takes the view expressed earlier that cyber terrorism can be viewed as hacking with political intent, then techniques used for hacking could also be used in cyber terrorism. As such, we divided the category of Intent into two categories – one more strongly related to cyber terrorism, and the second more strongly related to general hacking.

The terminology of cyber terrorism is not a well established and may vary from author-to-author. For this reason, a set of keywords was developed to characterize each of the major categories. The keyword list was developed after reviewing web sites devoted to cyber terrorism (Tables 2 and 3) and as such may not reflect general security concerns, but those that were most often mentioned in the context of cyber terrorism.

Table 2: Web sites used to develop keywords

http://www.geneva-link.ch/pgalley/infosec/sts_en/terrinfo.html
http://www.geneva-link.ch/pgalley/infosec/sts_en/iw.html
http://www.nautilus.org/info-policy/workshop/papers/denning.html
http://www.csis.org/pubs/cyberfor.html
http://afgen.com/terrorism1.html
http://abcnews.go.com/sections/world/DailyNews/chinahackers_010426.html
http://news.bbc.co.uk/1/hi/sci/tech/308788.stm

Table 3: Cyber terrorism categories and keywords

Intent (Cyber terrorism)

- Cyber/computer terrorism
- Information warfare
- Cyber/computer warfare
- Cyber/computer spies
- Cyber/computer saboteurs
- Cyber/computer espionage
- Cyber/computer defense
- Critical system/infrastructure disruptions

Intent (Hacking)

- Hacktivism
- Cyberactivist
- Computer network disruptions
- Service disruptions
- Internet-wide disruptions
- Communications disruption

Infrastructure

- Telecommunications
- Banking and finance
- Electrical power
- Oil and gas distribution/storage
- Water supply
- Transportation
- Emergency service (911)
- Government services

Techniques

- Malicious Code (Malware)
- Network attacks
- Viruses
- Worms
- Trojan horse
- DDOS/DDOS attacks
- Email viruses

As for the targets of cyber terrorism, Garrison (2003) mentions weapons of mass destruction and weapons of mass disruption as methods to cause damage to the infrastructure of a society. The President's Commission on Critical Infrastructure Protection identified eight infrastructures that constitute the life support systems of the nation. Each of these targets can be threatened by cyber terrorism; hence, they were included as keywords in that category.

The textbook analysis began with a review of the table of contents for references to the issues under study. Topics that receive significant coverage in a textbook warrant a citation in the table of contents as a chapter or section title (K. Bachrach, personal interview, November 2003). Therefore, if any of the keywords within a category were found in the table of contents, the text was noted as having an index entry for that category. Following the review of the table of contents, a similar analysis using the keywords was used for the index. The index of a textbook is designed to provide the reader easy access to the subjects presented in the book. A book designed to present information is faulty if it does not have proper indexing (Columbia, 2002). Thus, the strength of coverage of a specific topic can be gauged by the index citations of the topic.

Once the keywords for the table of contents and index citations were noted, the text analysis proceeded to review the relevant chapters or sections. A simple page count for each of the keywords was established as a rough measure of the extent of the coverage, and the keyword page counts were totaled for each category. Next, the researchers evaluated the text material and rated the coverage on a five-point Likert scale. The Likert scale served to establish a rating of the depth and completeness of the coverage as perceived by the research team. The team conducting the text analysis was looking for a viable presentation of the key issues of cyber terrorism with a depth sufficient to provide faculty and students with a foundation for further study. Therefore, an important factor in the text analysis was the inclusion of material that could form the basis for class discussion. The researchers hoped to find a depth of coverage that allows students to come to an understanding of the level of threat posed by cyber terrorism and a consideration of preventive measures.

Findings - Textbook Analysis

Table of Content Citations

The results for the analysis of the Table of Content (TOC) citations are shown in the first row of Table 4. The frequency of citations in the table of contents is somewhat encouraging. This statistic represents an effort to at least recognize the importance of this issue for future IT professionals. Terms in the intent category for cyber terrorism are found in the index of 75% of the textbooks in this study. The actual term "cyber terrorism" or "terrorism" appeared in the table of contents in 19% of the texts. Terms related to hacking are found in the index of 69% of the textbooks in this study. The terms for infrastructure targets did not appear at all in the main table of contents of any of the texts, though one of the books has more detailed contents listed at the start of each chapter – and some infrastructure targets are mentioned within that chapter table of contents. The techniques are frequently the focus of these security texts, and that is demonstrated by the fact that terms related to techniques appear in 88% of the texts.

Table 4: Results of textbook analysis

	Terrorism	Hacking	Targets	Techniques
TOC Citations	75%	69%	0%	88%
Index Citations	75%	69%	31%	94%
Mean Page Counts	8.50	2.38	1.50	35.86
Depth of Coverage	0.98	0.47	0.33	2.34

Index Citations

The results for the analysis of the Index citations are shown in the second row of Table 4. The frequency of citations in the index shows a similar pattern to that of the table of contents. Keywords related to cyber terrorism intent appeared in 75% of the textbooks in this study. Keywords related to hacking intent appeared in 69% of the textbooks. The actual term cyber terrorism or terrorism appeared in the table of contents of 44% of the texts. Note that 31% of the texts mention of infrastructure targets – mostly influenced by the one text that had the infrastructure keywords mentioned in the detailed table of contents. Techniques are cited in the index of 94% of the texts.

Mean Page Counts

Row three of Table 4 shows the results for the analysis of the mean page counts. The most number of pages on average was for techniques (35.86), which is consistent with our findings with the table of contents and index citations. The lowest average page count was for the infrastructure target category that received only 1.50 pages. The intent category for hacking at 2.38 was only marginally higher and intent (terrorism) earned a mean page count of 8.50. It is interesting to note that the terms related to the intent categories for cyber terrorism and hacking have on average less than 10 pages of coverage each.

Depth of Coverage

The results for the analysis of the coverage are shown in row 4 of Table 4. The depth of coverage for each category was rated on a Likert scale where 0 indicates no coverage and 4 indicates comprehensive treatment of a cyber terrorism category. Consistent with our earlier findings, techniques at 2.34 received the highest rating for all the categories. The terrorism category was second, rated at 0.98, well below the techniques category. The intent category for hacking was rated at 0.47 and the targets category at 0.33. Note that the average for coverage on techniques was

moderate and all of the other categories were rated at less than 1. This implies that though the texts mention terms related to cyber terrorism, there is very little in depth coverage provided.

Conclusion

Many MIS students take at most one course in computer security. Some of the hottest jobs in today's marketplace are related to computer security. Textbooks for courses in computer security provide a good foundation for the student to learn the techniques that are used to compromise computer systems and networks. However, this research suggests that computer security textbooks do not give cyber terrorism the depth of coverage warranted by its significance for the IT industry. The Department of Homeland Security clearly recognizes that cyber terrorism is a serious problem ("Threats and protection," n.d.). The scarcity of textbook coverage of cyber terrorism suggests that classroom coverage of the issue depends on the willingness of instructors to provide supplementary materials.

The finding of inadequate textbook coverage of cyber terrorism suggests the need for further research to uncover the extent of actual classroom coverage of this important issue by IT instructors. Questions for further research will include:

1. Is cyber terrorism discussed in the computer security course? How many schools offer such a course? How many business students take a security course?
2. Are MIS instructors supplementing the text with additional resources to provide more extensive coverage of cyber terrorism and related topics? If not, why not? If yes, what materials?
3. Do instructors and students have the same understanding of what the potential threats cyber terrorism represents?
4. Can a course on computer security adequately discuss the types of systems that control the major infrastructure targets and how they are vulnerable?
5. Why do computer security textbook authors and publishers believe it not important enough to provide more coverage? Is the issue too new and not well understood?

Interim Solution

Due to the inadequate coverage of cyber terrorism in most textbooks, instructors may want to supplement their course materials. Below is a list of websites and trade books that would be helpful sources of this information.

Websites

Dorothy Denning's Homepage, http://www.cs.georgetown.edu/~denning/index.html

Dorothy Denning has written numerous articles in the area of cyber terrorism. Her website provides links to many of her own publications as well as others. It also lists current activities and numerous web sites related to cyber terrorism.

Institute for Security Technology Studies (ISTS), http://www.ists.dartmouth.edu/ISTS/

The Institute for Security Technology Studies (ISTS) at Dartmouth College initiates interdisciplinary research and development projects addressing the challenges of cyber and homeland security. A search on the site for "cyber terrorism" returns over two hundred matches.

Computer Crime Research Center (CCRC), http://www.crime-research.org/

The Computer Crime Research Center is an independent institute with an international membership and dedicated to the research of cyber crime, cyber terrorism and other issues of computer crimes and internet fraud phenomena. The site has a good collection of recent news, articles, and events related to the broad area of computer crime, including cyber terrorism.

US Department of Homeland Security (DHS), http://www.dhs.gov/dhspublic/index.jsp

The United States Department of Homeland Security was established to protect the United States homeland and protect the American people. They provide the unifying core for the vast national network of organizations and institutions involved in efforts to secure the United States. The website provides some information on cyber terrorism, mostly as it relates to US homeland security.

US National Infrastructure Protection Center (NIPC), http://www.nipc.gov/

A division of the United States Department of Homeland Security that is focused on infrastructure protection and information analysis.

Council on Foreign Relations – Terrorism Questions and Answers – Cyberterrorism, http://www.terrorismanswers.org/terrorism/cyberterrorism.html

This site provides a good introduction to cyber terrorism through a question and answer format.

National Conference of State Legisatures – Cyber Terrorism, http://www.ncsl.org/programs/lis/CIP/cyberterrorism.htm

This website documents the efforts by United States state legislatures to address cyber terrorism.

United States Senate Judiciary Committee - Subcommittee on Terrorism, Technology and Homeland Security, http://judiciary.senate.gov/subcommittees/technology.cfm

This United States Senate subcommittee website has links to some interesting hearings related to cyber terrorism. Use the search feature in the “Hearings” section of the site to find interesting senate testimony on cyber terrorism.

Bitpipe, Inc. – CyberTerrorism Reports, http://www.bitpipe.com/rlist/term/Cyberterrorism.html

Bitpipe, Inc. provides access to a number of reports and white papers from various vendors on the subject of cyber terrorism.

Terrorism Research Center (TRC), http://www.terrorism.com

The Terrorism Research Center, Inc. is an independent institute dedicated to the research of terrorism, information warfare and security, critical infrastructure protection and other issues of low-intensity political violence and gray-area phenomena. This website provides resources for the general topic of terrorism.

Center for Strategic and International Studies (CSIS), http://www.csis.org/

The Center for Strategic and International Studies provides strategic insights on — and policy solutions to — current and emerging global issues. The site includes a few articles on cyber terrorism that can be found using the search feature.

Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress - Congressional Research Service Report, http://www.fas.org/irp/crs/RL32114.pdf

This report discusses possible cyber capabilities of terrorists and sponsoring nations, describes how computer security vulnerabilities might be exploited through a cyber terror attack, and raises some potential issues for Congress (from the report summary).

Trade books

"The Next War Zone: Confronting the Global Threat of Cyberterrorism" by James F. Dunnigan, Osborne/McGraw-Hill; 2002, ISBN: 0806524138.

"Critical Infrastructures" by Mathew T. Cogwell, Nova Science Publishers; 2002 ISBN: 1590333284.

"Protecting Your Enterprise from the New Global Threats of Terrorism; Cyber Terrorism and Infrastructure Attacks A- Plan of Action for Survival and Buisness Continuity in The New Global Threat Enviroment" by J.F. Kuong & Masp Consulting Group, MASP Consulting Group, J. Kuong, Management Advisory Publications, 3rd edition 2002, ISBN: 0940706571.

"Cybercrime and Cyberterrorism: Current Issues" by John V. Blane, Nova Science Publishers Inc.; 2003, ISBN: 1590337115.

"Black Ice: The Invisible Threat of Cyber-Terrorism" by Dan Verton, McGraw-Hill Osborne Media; 1st edition 2003, ISBN: 0072227877.

"Cyber Terrorism: A Guide for Facility Managers" by Joseph F. Gustin, Marcel Dekker Publisher; 2003, ISBN: 0824742915.

"Implementing Homeland Security for Enterprise IT" by Michael Erbschloe, Elsevier Digital Press; 2003, ISBN: 1555583121.

References

The Columbia Encyclopedia. (2003). Retrieved September 10, 2003, from http://www.bartleby.com/65/te/terroris.html

Council on Foreign Relations. (n.d.) Terrorism: An introduction. Retrieved September 22, 2003, from http://www.terrorismanswers.com/terrorism/introduction.html

Denning, D. (1999). Activism, hacktivism, and cyber terrorism: The Internet as a tool for influencing foreign policy. Retrieved October 10, 2003, from http://www.nautilus.org/info-policy/workshop/papers/denning.html

Denning, D. (2000a, May 23). Cyberterrorism. Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives Retrieved October 10, 2003, from, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

Denning, D. (2000b, September). Hacktivism: An emerging threat to diplomacy. Retrieved November 2, 2003, from http://www.afsa.org/fsj/sept00/Denning.cfm

Galley, P. (1996, May 30). Computer terrorism: What are the risks? [English translation July 1, 1998 by Arif M. Janmohamed]. Retrieved November 2, 2003, from http://www.geneva-link.ch/pgalley/infosec/sts_en/terrinfo.html

Garrison, A. H. (2003). Terrorism: The nature of its history. *Criminal Justice Studies. 16* (1), 39-52.

Hildreth, S. (2001, June). Cyberwarfare. [CRS Report for Congress]. Retrieved November 10, 2003, from http://www.fas.org/irp/crs/RL30735.pdf

Hirsch, E. Jr., Kett, J. & Trefil, J. (2002). *The new dictionary of cultural literacy* (3rd ed.). Boston: Houghton Mifflin.

Hummel, M. (n.d.). Cyberterrorism is a concern. Retrieved November 10, 2003, from http://www.crime-research.org/news/2003/02/Mess1701.htm

Kraft, D. (2000, October 26). Islamic groups 'attack' Israeli web sites. Retrieved November 10, 2003, from http://www.landfield.com/isn/mail-archive/2000/Oct/0137.html

Kulm, G., Roseman, J. E., & Treistman, M. (1999). A benchmarks-based approach to textbook evaluation. *Science Books & Films, 35*(4), 147-153. Retrieved January 12, 2004, from http://www.project2061.org/newsinfo/research/textbook/articles/approach.htm

Leif, D. J. (1994). Textbook treatment of structured programming standards and guidelines. *Journal of Information Systems Education, 6* (2).

MacDonald, L. & Fougere, K. (2003). Software piracy: A study of the extent of coverage in introductory MIS textbooks. *Journal of Information Systems Education, 13*, 325-329.

McWethy, J. & Starr, B. (2001, April 26). Hacker alert: Pentagon braces for Chinese computer attacks. Retrieved November 2, 2003, from http://abcnews.go.com/sections/world/DailyNews/chinahackers_010426.html

Nuttall, C. (1999, April 1). Kosovo info warfare spreads. Retrieved November 2, 2003, from http://news.bbc.co.uk/1/hi/sci/tech/308788.stm

Threats & Protection - Synthesizing and Disseminating Information. (n.d.) Retrieved April 10, 2004, from http://www.dhs.gov/dhspublic/theme_home6.jsp

Schneier, B. (2000). Semantic network attacks. *Communications of the ACM, 43* (12), 168.

Schwartau, W. (1994). *Information warfare: Chaos on the electronic super highway*. New York: Thunder's Mouth Press.

Vatis, M. (2001, September 22). Cyber attacks during the war on terrorism: A predictive analysis. Retrieved November 2, 2003, from http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_a1.pdf

Vatis, M. (2002, June). Cyber attacks: Protecting America's security against digital threats. Discussion paper ESDP-2002-04, John F. Kennedy School of Government, Harvard University.

Biographies

Janet J. Prichard is an assistant professor of computer information systems at Bryant University. She primarily teaches programming, data structures, and web development. She has also authored two data structures textbooks with Frank Carrano. Her research interests include web-based systems development, security, and spyware.

Laurie E. MacDonald is a professor of computer information systems at Bryant University. He has more than 35 years experience in information processing as a programmer, analyst, manager, and has taught for the past 25 years.