AU/ACSC/CHARGUALAF/AY08

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

TERRORISM

AND

CYBERCRIME

by

Joseph Chargualaf, Jr., Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: LTC John H. Anderson, III

Maxwell Air Force Base, Alabama

May 2008

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
MAY 2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Terrorism and Cybercrime	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air Command and Staff College Air University,Maxwell AFB,AL**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**36**	

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the U.S. government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Page

Preface

This research paper is an extension of my previous undergraduate studies in Criminal Justice and Terrorism and graduate-level studies in Information Systems. It allowed me to explore both issues in a topic relevant to the ongoing Global War on Terror. It is my hope that this paper in some way is able to contribute to our eventual victory in this endeavor

.

Abstract

Since 11 Sep 02, and the beginning of the declared U.S. War on Terror, modern terrorists increasingly rely on the Internet to conduct daily operations. They can no longer openly conduct meetings, recruit new members, train, and raise funds without the threat of U.S. attack. They were forced to adapt and have since successfully leveraged Internet capabilities to carry out their missions. They have proven their skills in spreading propaganda to shape public opinion and gain support from sympathizers. However, what is not as well publicized is their use of the Internet to conduct cybercrimes such as identity theft and credit card fraud for the express intent of raising funds in support of terrorist activities. The U.S. must adapt to these techniques and develop counter-measures with the same level of effort as when they froze assets in large financial institutions believed to belong to terrorists and their supporters.

The methodology utilized for this research paper is Problem/Solution. The problem is identified through the research and analysis of numerous periodicals and online articles. The solution is sought by interpreting legal documents, analyzing the roles of responsible organizations, exploring Internet technologies, and understanding ideologies leading to the establishment of terrorist organizations.

Introduction

Using al-Qaeda as an example, this research paper examines whether the United States is doing enough to defeat terrorist organizations organized around decentralized terrorist cells that use the Internet for criminal activity in order to raise funds for terrorist operations. This recent phenomena is driven by a number of factors; the dismantling of large terrorist organizations and the deaths of many of their key leaders, the freezing and seizing of terrorist related assets, the accessibility and the ease of using the Internet, and the opportunities for profitable crimes within the cyber domain.

Present day al-Qaeda is a much different organization than it was before the World Trade Center and Pentagon attacks on September 11, 2002 (9/11). Understanding the difference is important to understanding their motives for turning towards the cyber domain to conduct terrorist related operations. In doing so it must be clearly understood that their focus is not necessarily towards conducting cyber terrorism, but rather leveraging cyber technologies such as the Internet to enable terrorist operations in the physical domain.

In light of significant efforts to combat global terrorisms, terrorist organizations and their related smaller satellite cells have proven quite resilient. They constantly adapt to antiterrorism efforts through the use of technology and innovation, even to the point where it can be argued they are actually thriving in the cyber domain. They have already successfully leveraged the Internet to manipulate public opinion and gain sympathy for their cause. They have also found ways to translate this cyber success into ways of generating revenue in support of real world operations.

Due to the ubiquitous nature of the Internet, countering this threat is no easy feat for U.S. law enforcement agencies. In order to level the playing field new terrorism and cyber-related

laws were established shortly after 9/11. The key to enforcing these laws is the establishment of domestic and international organizations and the partnerships they have with business and industry. Together, the relationship between law and law enforcement organizations is an extremely successful combination. However, the ability for them to quickly adjust to new strategies and technologies fielded by terrorists within the cyber domain will ultimately decide who wins the "Cyber War on Terror".

Cyberterrorism vs. Cybercrime

Cyberterrorism

In efforts to better understand the dynamic problem faced in combating terrorists and their use of the cyber domain, a distinction must first be made between cyberterrorism and cybercrime. The Federal Bureau of Investigations (FBI) defines cyberterrorism as "The 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."[1] This type of attack is only read about or seen in movies as there is yet to be a cyber attack by terrorists against non-combatants to date. An example of this type of attack is breaking into a computer system used to regulate the flow of water for a dam. During this act the perpetrator fully opens the dam allowing water to flow unregulated into populated areas causing mass flooding and seriously compromising lives and property.

These kinds of scenarios are often dramatized in news reports and terrorist capabilities are often exaggerated. However, the truth is these types of attacks take significant cyber skills, in-depth insider technical knowledge of the targeted industry, enormous amounts of planning, large sums of money, and a great amount of negligence of the part of the industry under attack.[2]

Using the dam as an example, a terrorist organization would need to first find someone with the computer and programming skills needed to penetrate the dam's computer security. To make this particular step even more difficult is the likelihood that the flow regulation portion of the dam computer system is "air gapped". In other words, there is no physical or wireless connection leading from the dam's internal network to that of an outside network. This means the perpetrator would need to access the dam computer system from within the dam's physical structure. Even if this occurred, once inside the system the perpetrator would require the needed expertise to know the sequence of commands required to manipulate the flow regulators and by-pass any security protocols established to prevent dangerous flow patterns. This type of attack is extremely risky and requires a significant amount of insider knowledge to execute. The cost needed to employ the required technical expertise for this complex job would also prove very expensive to maintain. Finally, the probability of success is extremely low given the physical security of the dam first needs to be breached, and in all likelihood there are other dam technicians on duty specifically responsible for monitoring the vital statistics of dam operations. Should this potential "flood" scenario occur, technicians are trained to quickly mitigate these specific problems as they routinely practice for these types of disaster scenarios.[3]

This example demonstrates the complex nature of accomplishing such a cyber attack. It is far easier for a terrorist group to plan and execute a physical attack on a dam than it is to compromise it through the cyber domain. The complexities and low probability of success in executing cyberterrorism are the most significant factors as to why terrorist do not choose this method of attack. Rather, they choose direct physical attacks that prove more effective in accomplishing their objectives.[4] Physical attacks may also achieve the secondary effects of instilling fear and publicizing a cause even if the first level effect of causing a disaster scenario is

not achieved. It is not that terrorist do not want to use cyber attacks as a method of achieving their goals, it is just that they currently do not have the capabilities required to effectively do so.[5] Government and industry must continue to evolve security measures to ensure these capabilities are never achieved.

Cybercrime

Due to the nature of crime and how it is defined differently from one international culture to the next, it is currently impossible to find a common standardized definition of cybercrime.[6] This paper uses the definition provided by an international computer security giant, the Symantec Corporation, which derives its definition by including elements of the definition from entities such as The Council of European Unions and the United Nations. As such, Symantec defines cybercrime as "any crime that is committed using a computer or network, or hardware device."[7]

Given this definition, the cyber attack on the dam is considered a cybercrime since terrorism is a crime and the method used to employ it is via a computer network and associated hardware. This paper, however, focuses more on how terrorist are using the types of crimes usually committed by the typical "cyber thief" and less on actually committing a terrorist attack through the cyber domain. Specific cybercrimes are discussed later in this paper.

Al-Qaeda: Organization and Operations Past and Present

Pre-9/11

Before al-Qaeda attacked the WTC and Pentagon on 9/11, they essentially operated in an open environment without fear of attack from a formidable foreign power, especially the U.S.[8] Although aware of al-Qaeda's terrorist activities overseas the U.S. did not feel threatened by their existence. For the most part al-Qaeda was just another terrorist organization not unlike

other Islamic fundamentalist groups such as Hezbollah and HAMAS. Aside from the first bombing of the WTC in 1993, no other major terrorist attacks by a foreign agent had occurred within the continental U.S.[9] The threat for the most part seemed very far away and a problem for other countries to solve. The global influence of terrorism at the time was minimal and activities were isolated only to specific regions. As a result very little U.S. effort and resources actually went into combating terrorism.[10]

This opened the door for Osama Bin Laden to ally himself with the ruling Afghani government, the Taliban, in an effort to build a safe haven for the al-Qaeda organization. Building this relationship came at a high cost for Bin Laden as it is estimated he paid approximately $20 million a year to the Taliban government in exchange for sanctuary.[11] The relationship became so close that an outsider's perspective typically associated Bin Laden more with the Taliban than with al-Qaeda.

Within the Afghanistan sanctuary Bin Laden was able to build up the leadership of al-Qaeda while training prospective members to carry out the mission of the organization. The safe haven afforded al-Qaeda the opportunity to openly gather to conduct training and plan future operations.[12] It also allowed them to openly solicit and receive funds to support their organization and associated operations. During the five year period leading up to 9/11 they produced approximately 70,000 graduates and planned the attacks on the East Africa embassy, the U.S.S Cole docked in Yemen, and the WTC and Pentagon. Without the sanctuary provided them by the Taliban these attacks may not have been possible.[13]

The state sponsored sanctuary also enabled Bin Laden to establish an organized chain of command allowing him and his appointed leaders to centrally manage operations. The ability to meet face-to-face with his leaders ensured his intent was understood and missions were planned

without confusion.[14] This quickly changed after the attacks on 9/11.

Post 9/11:

Early in the War on Terror the United States was successful in decapitating the command and control of al-Qaeda. They hunted down and either killed or captured the majority of al-Qaeda's top leadership and destroyed most of the known training camps in Afghanistan soon after the WTC and Pentagon attacks on 9/11 forcing al-Qaeda to retreat "underground".[15] However, what may have appeared to be success in the beginning quickly turned to a new kind of war.

Al-Qaeda shifted tactics and began fighting asymmetrically, not only physically, but also in the cyber domain. Physically they used terrorist tactics and incited insurgencies by encouraging and participating in civil uprisings against the U.S. and allied forces and their interests. In the cyber domain they leveraged web-based tools to replace a once centralized command and control structure. Recently disconnected al-Qaeda members were again able to communicate and pass information over the Internet.[16]

Today al-Qaeda has come a long way and now has a strong web-based presence with capabilities that allow the sharing of strategy, intelligence, and training information. The cyber domain allows them to transcend the need for physical leadership and they now operate in a decentralized fashioned united as a collective via shared extremist ideology.[17] Although the frequency of terrorist attacks have actually gone up since 9/11, these attacks are relatively small in scale and evidence suggests they are conducted by localized independent terrorist cells vice large international terrorist organizations.[18]

Financing Al-Qaeda

Funding Needs

With this new decentralized structure comes a new problem for the U.S. Under the previous centralized organization, al-Qaeda was able to raise and solicit funds openly and transfer those funds through legitimate financial institutions without fear of retribution. The international response post-9/11 to seize and freeze finances linked to terrorist organizations caused significant impact to al-Qaeda's ability to fund major terrorist activities such as 9/11, estimated at $500,000.[19]

The importance of these funds to terrorist operations cannot be over emphasized. Terrorist organizations must not only pay for the direct costs of an attack (Figure 1),[20] but also operating costs much like any legitimate business. According to the 29 Feb 08 Financial Action Task Force (FATF) report on Terrorist Financing these cost include the following elements:

1) Salaries, subsistence, and communication: These costs include paying operatives to cover daily expenses including money to care for their families. Additional expenses are also derived from the need to establish communications.
2) Training, travel, and logistics: Self explanatory costs. Also includes the cost to obtain false identification needed for travel.
3) Shared funding: A terrorist cell belonging to a larger organization may feel compelled or be required to share funding with other cells within the organization in efforts to achieve objectives central to the overall organization.[21]

Figure 1. Direct Attack Costs of a Terrorist Conspiracy

Attack	Date	Estimated cost[3]
London transport system	7 July 2005	GBP 8 000[4]
Madrid train bombings,	11 March 2004	USD 10 000
Istanbul truck bomb attacks,	15 & 20 November 2003	USD 40 000
Jakarta JW Marriot Hotel bombing	5 August 2003	USD 30 000
Bali bombings	12 October 2002	USD 50 000
USS Cole attack	12 October 2000	USD 10 000
East Africa embassy bombings,	7 August 1998	USD 50 000

Source: Adapted from the Aug 04 report on Terrorist Attacks Upon the United States

In addition to these operational costs there are also broad organizational requirements that must be funded. These requirements include the need to spread propaganda in support of their cause. This is critical for sustaining current membership and recruiting new members who are sympathetic to their movement. Funds may also be required to sustain legal fronts such as a business or charity which are actually used to move funding through the terrorist network. These requirements in many cases are by far the largest funding drain on a terrorist organization.[22]

However, referring back to Figure 1 above, the overall cost to accomplish a single terrorist attack remains relatively low in relation to the strategic effect they cause in favor of the attacker. Not only does it instill fear in the attacked population, but it also draws attention to the cause of the terrorists, drives political policy, and forces countries to invest millions of dollars into security infrastructures designed to deter future attacks. The strategic effect afforded to the terrorist is in terms of expended time, manpower, and resources by the impacted governments, and perhaps even affords terrorist organizations a little breathing room to reconstitute.

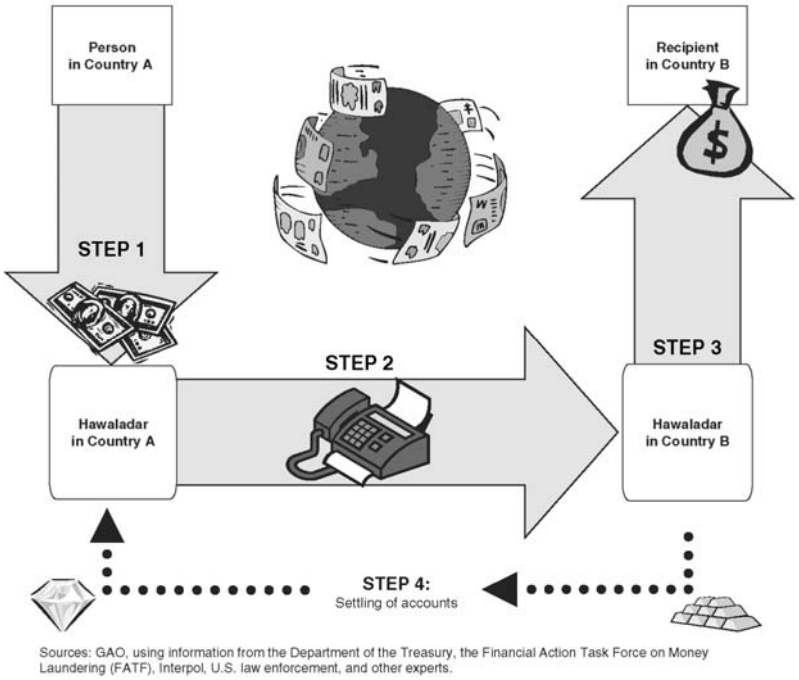
Shifting Strategies

New U.S. and international financial laws and regulations also make it difficult for al-Qaeda to transmit funding to smaller terrorist cells around the world.[23] Thus, smaller al-Qaeda operations are monetarily cut off from their mother organization and must find improvised ways

of generating revenue. Increasingly these smaller cells must turn to traditional criminal activities, including cybercrime, to obtain the necessary funding to carry out operations.[24] Examples of criminal activities engaged in by terrorists include the trading and selling of drugs, counterfeiting, and identity theft. Subsequently many of them are successful enough to find themselves financially independent of their larger organizations and are now in the position to make operational decisions on their own. This makes it increasingly more difficult for law enforcement to track and capture these terrorists.

Concealment of funds is done through the use of charities, informal banking systems, money laundering through legitimate shell companies, and commodities such as precious stones and metals.[25] They even have a well established, and well known, cash courier system designed to thwart technological detection by law enforcement called Hawala (Figure 2).

Figure 2. Hawala-type Transaction



In the scenario shown in Figure 2 Person A wants to transfer money to Person B in

another country. He takes the money to a Hawaladar in Country A who then contacts a Hawaladar in Country B to authorize release of the money to Person B. The Hawaladars in both countries then settle their accounts utilizing the concealment techniques described in the beginning of this paragraph. Given the nature of this person-to-person transaction it is essentially immune to detection by technological surveillance systems.[26]

Given the enormous profits generated by criminal activities, evidence suggests al-Qaeda will only increase its involvement in these areas. A report released in 2003 by the U.S. Drug Enforcement Agency (DEA) found that "14 of the 36 groups found on the U.S. State Departments list of foreign terrorist are involved in drug trafficking." As a result the DEA suggests that the war on terror and the war on drugs should be linked.[27] This is very strong evidence that terrorists are embracing alternative methods for raising funds, even if the methods used do not directly support their religious beliefs. This causes yet another dilemma for law enforcement officials as it makes it that more difficult to predict terrorist behaviors that fall outside their established profiles.

For comparative purposes the United Nations estimated the profits from the global drug trade to be approximately $322 billion per year in 2003. At its peak, the highest estimate for al-Qaeda's income is somewhere in the range of $1 billion.[28] These are high expectations for any criminal organization to achieve, much less smaller terrorist cells. Therefore, this paper only examines more modest and attainable methods of raising funds, specifically those acquired via the cyber domain. It is still important, however, to identify how terrorist organizations raise funds outside the cyber domain and the challenges they face when doing so to understand why they are increasingly turning to cybercrime as an alternate financial mechanism. Figure 3 reflects additional non-cyber related financing mechanisms used to earn, move, and store

assets.[29]

Figure 3. Alternative Financing Mechanisms

Examples of Alternative Financing Mechanisms That May Be Used to Earn, Move, and Store Terrorist Assets			
Alternative financing mechanisms	**Earning**	**Moving**	**Storing**
Trade in commodities			
Illicit drugs	X		
Weapons	X		
Cigarettes	X		
Diamonds	X	X	X
Gold		X	X
Systems			
Charities	X	X	
Informal banking		X	
Currency			
Bulk cash		X	X

Sources: GAO analysis based on government, industry, and research sources.

Terrorist in Cyberspace

So what makes cybercrime, particularly the use of the Internet, so compelling to terrorists? In an attempt to answer this one must turn to the particular characteristics of the Internet and explore assumptions as to its possible uses. Together these elements help explain why cybercrime has become a financial mechanism for terrorists.

Characteristics of the Internet

The Internet enables rapid, almost instantaneous, communication. This allows for easy sharing of information such as intelligence, planning, and the transfer of funds. It essentially creates a virtual environment to conduct business in real time without the need to physically gather.[30]

It is also a very inexpensive medium. One must only have access to the Internet to utilize free web-based services designed specifically for sharing information. These free services are provided by Fortune 500 companies such as Google, Yahoo, and Microsoft without any

verification of personal identity.[31]

Emerging user-friendly technologies coupled with the increasing amount of bandwidth also makes it easier for average users to generated sophisticated web-based products with very little effort. Terrorist now have the ability to produce professional-level websites with complicated interfaces that include features such as video. This makes it possible for even the most casual user to develop websites that before could only be accomplished by the most advanced web-based programmers.[32]

The key to making this all work is the ability to secure and mask data and identities in the cyber domain. This is accomplished using readily available and often times free encryption and anonymizer technologies which allows users to secure data they transmit over the Internet while at the same time disguising their origins.[33]

Perhaps the most important characteristic is the ubiquity of the Internet. It essentially allows terrorist organizations to operate on a global basis without the added requirement for physical infrastructures and personnel.[34] This is actually the biggest advantage terrorist organizations currently have since it allows them to communicate their message to decentralized cells around the world in efforts to ensure terrorist operations are conducted in support of the greater intent. It also allows them to establish successful information operation campaigns against the U.S. and its allies through the publishing of tightly controlled information on various web pages. They do this in efforts to discredit U.S. reports of success and progress in the War on Terror by publishing text, video, and photos contrary to U.S. claims.[35] Often times, however, the information is fabricated or misrepresented.[36] A good example of this is when several websites and news agencies reported that U.S. bombs hit a village destroying several homes and killing innocent civilians. It was later discovered that different photos used in the reports showing

women agonizing in front of their destroyed homes was actually the same woman staged in front of different buildings that had apparently already been destroyed during attacks occurring much earlier in the conflict.

Assumptions

According to a research paper written by three Air War College students titled *Flying and Fighting in Cyberspace*, the following assumptions can be made in regards to the current conditions of the cyber domain:

- Information-technology infrastructure is indispensable to public and private sector activities across the globe
- Interconnectivity exposes previously isolated critical infrastructure to risk of cyber attack
- Exposure to attacks is expected to rise as interconnectivity between technological devices increases
- Resources needed to conduct harmful attacks are readily available and inexpensive
- Adversaries are capable of launching harmful attacks on cyber dependant U.S. systems
- Geographic and national boundaries do not limit attacks in the cyber domain
- Sensitive information tends to be isolated from the Internet, however, means exist to breach these systems through various security weaknesses in gateways
- Protecting U.S. interests in the cyber domain is a matter of national and homeland security[37]

The combination of Internet characteristics and the assumptions identified above demonstrate that almost any entity determined to utilize the Internet for illegal purposes can easily do so if desired. The Internet provides a medium conducive to criminal activity that the physical domain does not provide. Operations in the cyber domain can quickly be established with very little cost while at the same time providing a potentially large rate of return. If

operations are discovered or become too risky, the cybercriminal can simply shut down operations and relocate elsewhere in the cyber domain using a different identity.

Threat Agents

Before discussing how terrorists are using the Internet to conduct specific cybercrimes, different types of cyber threat agents must first be identified and distinguished. The authors of *Flying and Fighting in Cyberspace* provide a summery of these threat agents in Figure 4.[38]

Figure 4. Threat Agents

Threat Agent	*Methodology*	*Intent*
Hackers	☒ Develop/use damaging code to break into private networks	☒ Malicious or criminal intent Theft, fraud, denial of service, and extortion
Organized crime	☒ Exploits online activity, hires hackers, bribes insiders Uses more structure/resources than hackers	☒ Monetary gain
Terrorists	☒ Hacking Exploitation of Internet	☒ Acquire information for planning physical or cyber attacks C2
Nation-states	☒ Offensive cyber capabilities Technical and operational capabilities for widespread impact limited to only a few	☒ Espionage Cyber warfare

Source: Office of Homeland Security, *National Strategy for Homeland Security* (Washington, DC: Government Printing Office, July 2002), passim, http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf.

Particular attention must be paid to the distinction made between organized crime and terrorist organizations. Although the methods and intent between organized crime when compared to terrorist are distinctly different, the reverse of this cannot be argued, however. The line between terrorist and the use of organized crime tactics have become extremely blurred, and in many cases no longer exist. As with the physical domain, terrorist are now looking towards organized crime techniques to generate revenue. Of course this complicates law enforcement efforts in combating both terrorism and organized crime as they may become indistinguishable.[39] This makes it even more important to consider them one in the same when it comes to law enforcement efforts.[40]

Cybercrime: Financial Opportunities

Although traditional fundraising through charitable contributions remains the first choice for terrorist revenue generation, criminal activity, both physical and virtual, have become more prevalent within smaller decentralized terrorist cells.[41] Cybercrime in particular provides a significant cost-to-benefit ratio that many terrorist cells are exploiting to generate and transfer funds, and there is no limit to the methods available to accomplish this. This section focuses on some of the more common, and assessable, forms of cybercrime and the potential utility they bring to a terrorist operation.

Identity Theft

Identity theft is considered a springboard for many types of cybercrime. Identity theft occurs when someone steals another person's personal information without their knowledge. They then use this information to commit theft or fraud. Many times victims unwittingly give up their sensitive personal information thinking they are providing it to legitimate sources.[42] This happens, for example, when victims receive an email from an apparently legitimate company such as their banking institution telling them they need to update account information. The email is composed with real company logos and directs them to click on a link to take them to the required website. After clicking on the link they are directed to a fake website that looks identical to the real thing. They dutifully enter their personal information such as social security number, account number, password, PIN, etc. When done they click submit and the data is saved on the criminal's server ready to use as they see fit. This specific example is a technique known as phishing or spoofing.[43]

In a November 2007 speech given to Penn State Students by Robert S. Mueller, Director of the FBI, he sites a case where an infamous al-Qaeda sympathizer and supporter based out of

the United Kingdom known as "Irhabi 007" stole thousands of credit card numbers through elaborate phishing schemes. He then used the card numbers to purchase over $3 million in equipment needed for terrorist operations.[44] This is a good example of how a small group of people with small budgets and access to the Internet can make an enormous financial impact on terrorist organizations.

Credit Card Fraud

Although the average person does not usually associated "cybercrime" with credit card fraud, it is perhaps the most well known of all the cybercrimes. This is where a criminal acquires someone's credit card information and illegally uses it to make purchases online.[45] This cybercrime is particularly dangerous in terms of terrorist potential in that items purchased using stolen credit card information can be used directly for a terrorist attack. In addition to the "Irhabi 007" example above, an investigation into the 2002 Bali night club attack in Indonesia that killed 202 people and left 100 more injured[46] shows that it was partially funded using stolen credit card information.[47]

Software Piracy and Counterfeiting

Software piracy and counterfeiting are related in that they are both forms of copyright infringements; however, they differ in their execution. Software piracy is making an illegal copy of copyrighted software and distributing it either via physical media or over the Internet. Counterfeiting is not only copying the data but also its packaging in efforts to pass it off as an original.[48]

According to the Software & Information Industry Association (SIIA), a leading global advocate for protecting software copyrights, pirating and counterfeiting of copyrighted software costs the software industry approximately $11-12 billion in revenue annually. This statistic is

not only a good indicator of the pervasiveness of this type of cybercrime, but also the potential revenue generator for a terrorist operation.[49]

As an example, in Aug 2006 Nathan Peterson, the operator of one of the largest U.S.-based for-profit software piracy websites, was sentenced to six years in prison and given a $500,000 fine for illegally selling and distributing pirated and counterfeited software. Estimates show he distributed over $20 million worth of copyrighted software for a personal profit of $5.4 million in only two years. He used the profits to live a life of luxury, a terrorist on the other hand would have different intentions altogether.[50]

Auction Fraud

According to the Internet Crime Complaint Center (IC3), a partnership between the Federal Bureau of Investigations (FBI) and the National White Collar Crime Center (NW3C), auction fraud is the most widespread form of Internet crime today. This cybercrime involves the misrepresentation or non-delivery of items listed on an auction site such as eBay. Essentially a buyer makes a bid on an item and then pays for it. Then either the item arrives and is not what was described in the auction listing, or the item never arrives at all. By this time the seller has already collected the money and most likely disappeared from the auction site. The criminal is then free to re-establish another account under a new user name if he wishes. The victim's only recourse at this point is to submit complaints through the auction site and perhaps the IC3. Chances are, however, that the seller used false credentials and either had a PO Box or an out of country address making it almost impossible to identify the perpetrator.[51]

Counterfeit Cashiers Check

The counterfeit cashiers check concept is rather simple. It usually involves someone trying to sell an expensive item using online classified ads. The seller is contacted by someone

(the perpetrator) claiming to be interested in buying their item. The buyer then convinces the seller he has a friend who owes him money (usually in the U.S.) and then sends him a cashiers check (counterfeit) to not only cover the cost of the item, but also the cost to ship it out of country. The buyer explains the amount will be more than what is required and instructs the seller to wire the balance back to him once the check has cleared. Since the bank believes the payment is a legitimate cashiers check they clear it almost immediately. The seller believing the transaction is successful then wires the money to the buyer, sometimes in excess of $1,000, only to find out later that the check did not really clear. The seller is then responsible to the bank for the insufficient funds.[52]

Consequences

These examples are but a few types of cybercrime available to terrorists for revenue generation. They are all very real threats and in all likelihood already utilized by very tech-savvy terrorists. The younger generations of Islamic fundamentalists acquire many computer skills through current educational systems, some located in the U.S.[53] For skills not organically available to terrorist organizations, external expertise may be bought at a price. Such expertise is found in abundance in countries such as the former Soviet Union where high paying jobs are no longer available to skilled engineers, technicians, and programmers. Most of the time these hired experts are not even aware they are working for a terrorist organization.[54]

Given the high rate of financial return provided by cybercrime when compared to the relatively low cost of executing a terrorist act, the probability of smaller decentralized cells turning to the Internet and cybercrime is only likely to increase. How law enforcement agencies react to counter this threat will play a critical role in the overall War on Terror.

Countering the Threat

Uneven Playing Field

Combating terrorists' use of cybercrime is an epic challenge for law enforcement given the uneven playing field in the cyber domain. Unlike terrorist, law enforcement must play by rules set forth in law and policy designed to protect constitutional rights of law abiding citizens. Oftentimes criminals are made aware of law enforcement techniques and upcoming crack downs due to leaks announced by the media. For example, the media was the first to make public the FBI's use of a tool called Carnivore designed essentially to wiretap into Internet communications using a tool called Carnivore.[55] Not only did this let cybercriminals know they were vulnerable, but it created such an large outcry by the public, mostly driven by media reports, that privacy rights were being violated. Shortly after the Carnivore tool was discontinued, although many believe the real reason for abandoning the program was due to the U.S. Patriot Act and the increased authority given to law enforcement to track and intercept communications.[56] The PATRIOT Act is discussed in greater detail later in this section.

Identifying and capturing terrorist in the cyber domain is also increasingly difficult. They are more sophisticated and utilize powerful tools which allow them to remain anonymous.[57] They also practice a technique of constantly relocating websites from server to server essentially making it impossible to shut sites down. Proof of their sophistication is provided by their ability to break into government and industry servers and utilizing them to host their content.[58] They are also known to work in teams that essentially assign specific tasks of a cyber operation to different individuals possessing the required skill sets. To protect the integrity of operations they typically do not know the other members of the team. This team concept also allows them to integrate expertise outside the terrorist organization where internal expertise is short.[59]

PATRIOT Act

How do you counter such a dynamic threat? You start by changing and updating laws designed specifically to combat the threat. The U.S. did just this with the introduction of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, also known as the PATRIOT Act. The PATRIOT Act provides law enforcement with four essential advantages in combating terrorism:

- Allows investigators to use specific crime fighting tools to combat organized crime and terrorism.
- Facilitates the information sharing and cooperation between government agencies.
- Updates antiquated laws to address new technologies and threats.
- Increases the penalty for those who commit terrorism.

Together these elements of the PATRIOT Act take one step closer to leveling the playing field against cybercrime. Specific sections within the act directly aimed at battling cybercrime are identified below:

- Section 201 – *Authority to intercept wire, oral, and electronic communications relating to terrorism.* This section adds terrorism to the list of offenses for which it is valid to intercept communications. Probable cause, a court orders, and warrants are still required.
- Section 212 – *Emergency disclosure of electronic communications to protect life and limb.* Allows law enforcement access to the servers belonging to Internet service providers (ISP) if it is suspected information is resident which may prove useful during a terrorist emergency.
- Section 217 – *Interception of computer trespasser communication.* Essentially makes trespassing on someone's computer equivalent to physical trespassing. It gives law enforcement the authority to investigate such intrusions with the consent of the victim.

- Section 219 – *Single-jurisdiction search warrants for terrorism.* Establishes one warrant based on the crime rather than jurisdiction. Also law enforcement to cross jurisdictional boundaries during pursuit or investigation. This is critical to fighting cybercrime due to its ubiquitous nature.
- Section 220 – *Nationwide service of search warrants for electronic evidence.* Allows a court with authority over a specific crime to issue a search warrant for a ISPs server regardless of jurisdiction. Another key element to fighting cybercrime as the Internet crosses multiple jurisdictions.
- Section 319 – *Forfeiture of funds in United States interbank accounts.* Allows authorities to seize funds tied to terrorism deposited in another countries bank if they are part of an interbank system. This eliminates financial "safe havens" for terrorist funding.
- Section 373 – *Illegal money transmitting business.* Makes it illegal to run an unlicensed foreign money transmittal business. Eliminates a method for cybercriminals to transfer funds outside the country.
- Section 806 – *Assets of terrorist organization.* Amends federal forfeiture laws to authorize assets owned by persons engaged in terrorism.[60]

These sections provide law enforcement with the legal leverage to seek, monitor, and capture terrorists engaged in cybercrime. Before the establishment of the PATRIOT Act it was almost impossible for law enforcement to keep pace with criminals in the cyber domain due to the speed of which transactions occur. The PATRIOT Act reduced a significant amount of bureaucratic red tape and opened the door to unprecedented interagency and international cooperation. This cooperation is indispensable in fighting terrorism and cybercrime.

Organizations

Laws alone are not enough to fight and win the multidimensional battle against cybercrime. Organizations also play a key role in monitoring and enforcing these laws. The successful collaboration between government organizations, industry, and international partners can make the difference between success and failure. Fortunately, numerous steps have been taken to ensure the best possible chance for success.

The agency at the tip of the spear is the FBI who responded by creating a Cyber Investigations Division specifically charged with fighting cyber threats. The FBI's cyber mission is fourfold: 1) stop those behind the most serious computer intrusions and spread of malicious code; 2) identify and thwart online sexual predators; 3) counteract operations that target U.S. intellectual property; and 4) dismantle national and transnational organized criminal enterprises engaging in Internet fraud.[61] At the forefront of their operations are 92 Cyber Crime Task Force offices (CCTF) located throughout the country. The CCTFs employ a cadre of mixed skills ranging from FBI field agents, intelligence analysts, and computer experts. They even deploy 60 Legal Attachés around the world, who together with their international partners investigate international cyber threats.[62]

Since the Cyber Investigations Division is organized specifically to combat crimes committed in the cyber domain they are equipped with the latest expertise, technology, and tactics designed to stay one step ahead of terrorists and criminals using the cyber domain for illicit activities. This proactive approach is a change from previous strategies designed merely for defensive or reactionary purposes. Two recent examples indicating the success of the Cyber Investigations Division against cybercrime are listed below:

- Breaking up a massive online software, movie, music, and videogame pirating ring which

involved the collaboration of 30 field offices resulting in arrests in 11 countries.

- Capturing two identity thieves who stole credit card numbers through the use of phishing emails.[63]

Given the shear volume of cyber related crimes in the U.S. the FBI counts on partnerships with cyber-enabled business and industries, such as Microsoft and AOL.[64] These partnerships allows for a wide array of information sharing, that when put together and analyzed, gives the FBI the ability to link commonalities which may lead to capturing criminals. This strategy of "connecting the dots" cannot be accomplished without the cooperation and partnership with private organizations.[65]

The most successful of these partnerships is the National Cyber-Forensics & Training Alliance (NCFTA). The NCFTA is the first partnership of its kind. It marries the skills of subject matter experts from industry, business, and government. Is goal is to merge fragmented information from across public and private sectors into meaningful data that enables a proactive response against cyber threats.[66] Collaboration efforts between the FBI and the NCFTA have lead to the successful capture and prosecution of the most serious cybercriminals.[67]

Another notable FBI partnership mentioned earlier is the IC3. The IC3 is proving to be an extremely valuable tool in the fight against cybercrime. The IC3 is essentially an online clearing house for reporting both individual and business related cybercrime incidents.[68] It does not respond to complaints directly, but rather forwards them to appropriate law enforcement agencies for follow-on investigations. As with the NCFTA, the IC3's main strong point is the ability to analyze commonalities between seemingly distinctive incidents in efforts to identify potential linkages and trends. This allows law enforcement agencies to take proactive measures in fighting threats.[69]

Since cybercrime has no borders, international partnerships are extremely vital. Cybercrime is a major international threat, but the problem is the definition of what constitutes a crime differs from country to country. Therefore, the European Union (EU) established the Critical Information Infrastructure Research Coordination Office to review how member states are protecting their critical infrastructures. In addition, the Council of Europe created the Convention on Cybercrime, consisting of 43 countries, designed to standardize definitions and laws as they pertain to hacking, copyright infringement, computer fraud, child pornography, and other illicit online activities.[70] This effort shows the EU's commitment to fighting cybercrime and provides the U.S. with a formidable partner in the fight. Similar initiatives are also underway by other members of the United Nations.

The establishment of laws such as those driven by the PATRIOT Act combined with effective anti-cybercrime organizations has proven quite successful in recent history. Criminals are no longer able to hide behind antiquated laws and enforcement agencies are no longer tied up by unnecessary bureaucratic red tape. Not only are organizations more effective at finding and capturing cybercriminals, they are also better organized and equipped to meet the dynamic challenges they face in the cyber domain. The shift from a purely defensive posture to a proactive strategy has succeeded in leveling a once uneven playing field.

Recommendations

I initially chose this topic with the impression that the U.S. is not doing enough to combat the use of cybercrime by terrorist organizations as an alternate funding mechanism. Through my research, however, I found this is not actually the case. I was impressed by the shear effort put forth not only in the fight against terrorism, but also the clear understanding and strategies already in place to combat cybercrime. The inception of the PARTIOT Act not long after 9/11

lead the way for law enforcement agencies to affect major changes designed specifically to combat terrorism and their potential funding streams. This resulted in highly skilled and technologically equipped organizations designed to carryout the proactive strategies needed to counter a very dynamic cyber threat. It paved the way for innovative partnerships between private and public entities that serve as force multipliers for law enforcement. We may never beat the use of cybercrime by terrorist organizations altogether, however, they are no longer able to freely manipulate the cyber domain to meet their fund raising needs. My final conclusion is that raising funds in cyberspace today is actually just as difficult for terrorists as raising funds in the physical domain.

Conclusions

The fight against terrorism has evolved significantly since 9/11. Proof of this is seen in the drastic changes undertaken by al-Qaeda as they adapt to antiterrorism initiatives specifically designed to eliminate their existence. Unable to operate openly and struggling to fund operations, they are now effectively leveraging the cyber domain, in particular the Internet, to communicate leadership intent, distribute orders, execute information operation campaigns, recruit and train members, and generate revenue to carry out operations.

The Internet provides several advantages for terrorists not found in the physical world that are manipulating to their benefit. Given the decentralized nature of most modern day terrorist organizations and lack of funding mechanisms available to earn, transfer, and store money, they increasingly rely on the Internet for this purpose. Evidence shows they are turning to illicit online activities and are increasingly committing cybercrimes once reserved for organized crime and stereotypical thieves and fraudsters. This is an effective strategy given the potential profit of such crimes in relation to the relative low cost of executing a single terrorist

operation.

Terrorist utilizing the cyber domain are not left unhindered, however. They are challenged by equally sophisticated law enforcement agencies that are teamed which partners from business and industry. Their combined effort helps to solidify and enforce new antiterrorism and cyber-related laws such as those established by the Patriot Act. This has leveled a once uneven playing field and has made it much more difficult for terrorist to leverage the enormous profit potential found in the execution of cybercrimes.

NOTES

[1] SearchSecurity.com, "*Definitions: Cyberterrorism*."
http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci771061,00.html
[2] Lachow, Irving, Richardson, Courtney. "*Terrorist Use of the Internet: The Real Story*." Joint Forces Quarterly, iss. 45, 2d qtr 2007: 100-102, 100
[3] Green, Joshua. "*The myth of cyberterrorism: there are many ways terrorists can kill you—computers aren't one of them*." Washington Monthly. 34.11 (Nov 2002): 8
[4] Lachow. "*Terrorist Use of the Internet*.", 101
[5] Sebastian M. Convertino, II, Lou Anne DeMattei, Tammy M. Knierim. *Flying and Fighting In Cyberspace*. Maxwell AFB, AL: Air University Press, 2007, 26
[6] Symantec Corporation. "*What is Cybercrime?"*, 1
[7] Symantec Corporation. "*What is Cybercrime?*"http://www.symantec.com/norton/cybercrime/definition.jsp, 1
[8] U.S. Treasury Department. "*Progress in the War on Terrorist Financing: 2003 Report*." 11 September 2003. http://www.treas.gov/press/releases/reports/js721.pdf, 1
[9] InfoPlease.com, "*Terrorist Attacks*.", http://www.infoplease.com/ipa/A0001454.html
[10] *9-11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, 9-11 Commission. http://www.gpoaccess.gov/911/pdf/fullreport.pdf, 76
[11] Beyond al-Qaeda. 61
[12] Beyond al-Qaeda. 62
[13] Beyond al-Qaeda. 62
[14] Beyond al-Qaeda. 61
[15] Scherer, John L. "*The U.S.'s befuddled approach to the war on terrorism.(Worldview).*" U.S.A Today. (Nov 2004): 16, 1
[16] Jacobson, Michael. "Grading U.S. Performance Against Terrorism Financing." The Washington Institute for Near East Policy, 5 September 2007, http://www.washingtoninstitute.org/print.php?template=C05&CID=2656 (accessed 20 Nov 2007), 1
[17] Wilson, Clay. "Emerging Terrorist Capabilities for Cyber Conflict Against the U.S. Homeland." (Congressional Research Service of the Library of Congress, 1 Nov 2005), 6
[18] Beyond al-Qaeda. 16
[19] Beyond al-Qaeda. The Global Jihadist Movement. (The Rand Corporation, 2006), 64
[20] *Terrorist Financing*. Financial Action Task Force, 29 February 2008. http://www.fatf-gafi.org/dataoecd/28/43/40285899.pdf, 7
[21] *Terrorist Financing*. Financial Action Task Force, 8
[22] *Terrorist Financing*. Financial Action Task Force, 8
[23] Kaplan, Eben. "Tracking Down Terrorist Financing." (Council on Foreign Affairs, 4 Apr 2006), http://www.cfr.org/publication/10356 (accessed 20 Nov 2007), 2
[24] Beyond al-Qaeda. 60
[25] *Terrorist Financing: U.S. Agencies Should Systematically Assess Terrorists' Use of Alternate Financing Mechanisms*. GOA Report to Congress. Washington, DC: U.S. General Accounting Office, November 2003. http://www.gao.gov/new.items/d04163.pdf, 9
[26] *Terrorist Financing*. Financial Action Task Force, 29 February 2008. http://www.fatf-gafi.org/dataoecd/28/43/40285899.pdf, 18
[27] Wilson. "Emerging Terrorist Capabilities.", 13
[28] Beyond al-Qaeda. 59
[29] *Terrorist Financing*. GOA Report to Congress, 10
[30] Weinmann, Gabriel. "*How Modern Terrorism Uses the Internet.*" AsianTribune.com, 21 February 2007. http://www.asiantribune.com/index.php?q=node/4627
[31] Lachow. "*Terrorist Use of the Internet*.", 101
[32] Keefe, Patrick. Digital Underground. The Village Voice, 16-22 Feb 2005. Vol 50, Iss. 7, 14
[33] Nadya, Labi. Jihad 2.0, The Atlantic Monthly, July 1. 102-108, http://www.proquest.com/, 1
[34] Lachow. "*Terrorist Use of the Internet*.", 100
[35] Lachow. "*Terrorist Use of the Internet*.", 101
[36] Lachow. "*Terrorist Use of the Internet*.", 102
[37] Sebastian. *Flying and Fighting In Cyberspace*., 21
[38] Sebastian. *Flying and Fighting In Cyberspace*., 24

[39] Shelley, Louise. "Organized Crime, Terrorism and Cybercrime." Computer Crime Research Center, 27 Sept 2007, http://www.crime-research.org/articles/terrorism_cybercrime
[40] Wilson. "Emerging Terrorist Capabilities.", 13
[41] Mueller, Robert S., Director of the FBI. Address. Penn State Forum Speaker Series, State College, Pennsylvania, 6 November 2007 http://www.fbi.gov/pressrel/speeches/mueller110607.htm
[42] The Internet Crime Complaint Center. "*Internet Crime Schemes*.", http://www.ic3.gov/crimeschemes.aspx/
[43] The Internet Crime Complaint Center. "*Internet Crime Schemes*."
[44] Mueller, Robert S., Penn State Forum Speaker Series
[45] Wilson. "Emerging Terrorist Capabilities.", 11
[46] GlobalSecurty.org. "*Bali Nightclub Bombing*." http://www.globalsecurity.org/security/ops/bali.htm
[47] Wilson. "Emerging Terrorist Capabilities.", 4
[48] The Software & Information Industry Association. "*What is Software Piracy: The Piracy Problem*." http://www.spa.org/piracy/whatis.asp, 15
[49] The Software & Information Industry Association. "*What is Software Piracy.",* 1
[50] U.S. Department of Justice. "*For-Profit Software Piracy Website Operator Sentenced to 87 Months in Prison.*" http://www.usdoj.gov/criminal/cybercrime/petersonSent.htm
[51] The Internet Crime Complaint Center. "*Internet Crime Schemes*."
[52] The Internet Crime Complaint Center. "*Internet Crime Schemes*."
[53] Wilson. "Emerging Terrorist Capabilities.", 9
[54] Wilson. "Emerging Terrorist Capabilities.", 14
[55] CBS.com, "FBI's Carnivore Devours Criminals" http://www.cbsnews.com/stories/2001/05/04/archive/technology/main289590.shtml
[56] Doyle, Charles. *The U.S.A PATRIOT Act: A Sketch*. CRS Report for Congress, Congressional Research Service: The Library of Congress, 18 April 2002, CRS-1
[57] Wilson. "Emerging Terrorist Capabilities.", 9
[58] Nadya. Jihad 2.0, 1
[59] Shelley, Louise. "Organized Crime, Terrorism and Cybercrime."
[60] Preserving Life and Liberty. "The U.S.A PATRIOT Act: Myth vs. Reality" http://www.lifeandliberty.gov/subs/add_myths.htm
[61] Federal Bureau of Investigations. "Cyber Investigations." http://www.fbi.gov/cyberinvest/cyberhome.htm
[62] Farnen, James E., Director of the FBI Cyber Investigations Division. *House Committee Hearing on Government Reform; The FBI's Cyber Division*. 15 May 2003, http://www.fbi.gov/congress/congress03/farnan051503.htm
[63] Federal Bureau of Investigations. "*Netting Cyber Criminals: Inside the Connecticut Computer Crimes Task Force*." http://www.fbi.gov/cyberinvest/cyberhome.htm
[64] Swartz, Jon. "*Shhh, they're hunting cybercrooks: Sleuths hunker down to catch Net's most-wanted*." U.S.AToday.com, accessed 1 April 2008., http://www.usatoday.com/educate/college/careers/news15.htm
[65] Levitt, Matthew. "Blocking Terror Finances." The Washington Institute for Near East Policy, 3 May 2007, http://www.washingtoninstitute.org/print.php?template=C05&CID=2656
[66] National Cyber-Forensics & Training Alliance. "*About National Cyber-Forensics & Training Alliance*." http://www.ncfta.net/about.asp
[67] Martinez, Steven M., Deputy Director of the FBI Cyber Investigations Division. *House Committee Hearing on Small Business Regulatory Reform and Oversight Subcommitee*. 16 March 2006. http://www.fbi.gov/congress/congress06/martinez031606.htm
[68] Martinez, Steven M., *House Committee Hearing*
[69] The Internet Crime Complaint Center. "*About Us*." http://www.ic3.gov/about/
[70] Wilson. "Emerging Terrorist Capabilities.", 16

Bibliography

9-11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States, 9-11 Commission. http://www.gpoaccess.gov/911/pdf/fullreport.pdf

Beyond al-Qaeda. The Global Jihadist Movement. (The Rand Corporation, 2006)

CBS.com, "FBI's Carnivore Devours Criminals" http://www.cbsnews.com/stories/2001/05/04/archive/technology/main289590.shtml

Charette, Robert N., "*Financing Terrorism*." IEEE Spectrum. Accessed 1 Apr 2008 http://spectrum.ieee.org/print/5672

Doyle, Charles. *The U.S.A PATRIOT Act: A Sketch*. CRS Report for Congress, Congressional Research Service: The Library of Congress, 18 April 2002

Farnen, James E., Director of the FBI Cyber Investigations Division. *House Committee Hearing on Government Reform; The FBI's Cyber Division.* 15 May 2003 http://www.fbi.gov/congress/congress03/farnan051503.htm

Federal Bureau of Investigations. "Cyber Investigations." http://www.fbi.gov/cyberinvest/cyberhome.htm

Federal Bureau of Investigations. "*Netting Cyber Criminals: Inside the Connecticut Computer Crimes Task Force*." http://www.fbi.gov/cyberinvest/cyberhome.htm

Financial Action Task Force. "*9 Special Recommendations (SR) on Terrorist Financing (TF).*" http://www.fatf-gafi.org/document/9/0,3343,en_32250379_32236920_34032073_1_1_1_1,00.html

Financial Action Task Force. "*About the FATF*." http://www.fatf-gafi.org/pages/0,3417,en_32250379_32236836_1_1_1_1_1,00.html

Fulghum, David. "Digits of Doom: Cyberwar Is Underway." *Aviation Week & Space Technology*, vol. 167, Iss. 12, 24 September 2007, p. 74

GlobalSecurty.org. "*Bali Nightclub Bombing*." http://www.globalsecurity.org/security/ops/bali.htm

Green, Joshua. "*The myth of cyberterrorism: there are many ways terrorists can kill you—computers aren't one of them.*" Washington Monthly. 34.11 (Nov 2002): 8

InfoPlease.com, "*Terrorist Attacks*.", http://www.infoplease.com/ipa/A0001454.html

Jacobson, Michael. "Arab States' Efforts to Combat Terrorism Financing." The Washington Institute for Near East Policy, 16 April 2007, http://www.washingtoninstitute.org/print.php?template=C05&CID=2590

Jacobson, Michael. "Grading U.S. Performance Against Terrorism Financing." The Washington Institute for Near East Policy, 5 September 2007, http://www.washingtoninstitute.org/print.php?template=C05&CID=2656

Kaplan, Eben. "Tracking Down Terrorist Financing." (Council on Foreign Affairs, 4 Apr 2006), http://www.cfr.org/publication/10356

Kaplan, Eben. "Rethinking Terrorist Financing." (Council on Foreign Affairs, 31 Jan 2007), http://www.cfr.org/publication/12523

Keefe, Patrick. Digital Underground. The Village Voice, 16-22 Feb 2005. Vol 50, Iss. 7

Kohlmann, Evan. "The Real Online Terrorist." (Foreign Affairs, Sep/Oct 2006, vol. 85, Num 5)

Labi, Nadya. Jihad 2.0, The Atlantic Monthly, July 1. 102-108, http://www.proquest.com/

Lachow, Irving, Richardson, Courtney. "*Terrorist Use of the Internet: The Real Story*." Joint Forces Quarterly, iss. 45, 2d qtr 2007: 100-102

Levitt, Matthew. "Blocking Terror Finances." The Washington Institute for Near East Policy, 3

May 2007, http://www.washingtoninstitute.org/print.php?template=C05&CID=2656
Martinez, Steven M., Deputy Director of the FBI Cyber Investigations Division. *House Committee Hearing on Small Business Regulatory Reform and Oversight Subcommitee*. 16 March 2006. http://www.fbi.gov/congress/congress06/martinez031606.htm
Mueller, Robert S., Director of the FBI. Address. Penn State Forum Speaker Series, State College, Pennsylvania, 6 November 2007 http://www.fbi.gov/pressrel/speeches/mueller110607.htm
National Cyber-Forensics & Training Alliance. "*About National Cyber-Forensics & Training Alliance*." http://www.ncfta.net/about.asp
Preserving Life and Liberty. "The U.S.A PATRIOT Act: Myth vs. Reality" http://www.lifeandliberty.gov/subs/add_myths.htm
Scherer, John L. "*The U.S.'s befuddled approach to the war on terrorism.(Worldview).*" U.S.A Today. (Nov 2004): 16
SearchSecurity.com, "*Definitions: Cyberterrorism*." http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci771061,00.html
Sebastian M. Convertino, II, Lou Anne DeMattei, Tammy M. Knierim. *Flying and Fighting In Cyberspace*. Maxwell AFB, AL: Air University Press, 2007
Shelley, Louise. "Organized Crime, Terrorism and Cybercrime." Computer Crime Research Center, 27 Sept 2007, http://www.crime-research.org/articles/terrorism_cybercrime
Swartz, Jon. "*Shhh, they're hunting cybercrooks: Sleuths hunker down to catch Net's most-wanted*." U.S.AToday.com, accessed 1 April 2008. http://www.usatoday.com/educate/college/careers/news15.htm
Symantec Corporation. "*What is Cybercrime?*" http://www.symantec.com/norton/cybercrime/definition.jsp
Terrorist Assets Report: Calendar Year 2004, Thirteenth Annual Report to the Congress on Assets in the United States of Terrorist Countries and International Terrorism Program Designees. Office of Foreign Assets Control, Department of the Treasury http://www.treas.gov/offices/enforcement/ofac/reports/tar2004.pdf
Terrorist Financing. Financial Action Task Force, 29 February 2008. http://www.fatf-gafi.org/dataoecd/28/43/40285899.pdf
Terrorist Financing: U.S. Agencies Should Systematically Assess Terrorists' Use of Alternate Financing Mechanisms. GOA Report to Congress. Washington, DC: U.S. General Accounting Office, November 2003. http://www.gao.gov/new.items/d04163.pdf
The Internet Crime Complaint Center. "*About Us*." http://www.ic3.gov/about/
The Internet Crime Complaint Center. "*Internet Crime Schemes*." http://www.ic3.gov/crimeschemes.aspx/
The Software & Information Industry Association. "*What is Software Piracy: The Piracy Problem*." http://www.spa.org/piracy/whatis.asp
U.S. Department of Justice. "*For-Profit Software Piracy Website Operator Sentenced to 87 Months in Prison*." http://www.usdoj.gov/criminal/cybercrime/petersonSent.htm
U.S. Department of Justice. "*Reporting Computer, Internet Related, or Intellectual Property Crime*." http://www.usdoj.gov/criminal/cybercrime/reporting.htm
U.S. General Accounting Office. "Investigations of Terrorist Financing, Money Laundering, and Other Financial Crimes." http://www.gao.gov/new.items/d04464r.pdf
U.S. Treasury Department. "*Progress in the War on Terrorist Financing: 2003 Report*." 11 September 2003. http://www.treas.gov/press/releases/reports/js721.pdf

Weinmann, Gabriel. "*How Modern Terrorism Uses the Internet.*" AsianTribune.com, 21 February 2007. http://www.asiantribune.com/index.php?q=node/4627

Wilson, Clay. "Emerging Terrorist Capabilities for Cyber Conflict Against the U.S. Homeland." (Congressional Research Service of the Library of Congress, 1 Nov 2005)