White Paper

Center for the Study of
Terrorism and Irregular Warfare
Monterey, CA

Cyberterror

Prospects and Implications

December, 1999

Authors:
Major Bill Nelson, USAF
Major Rodney Choi, USMC
Major Michael Iacobucci, USA
Major Mark Mitchell, USA
Captain Greg Gagnon, USAF

Project Supervisors:
Dr. John Arquilla
Dr. David Tucker

Disclaimer

This study was prepared and produced at the Naval Postgraduate School. The views expressed in this report are those of the authors and do not reflect the official policy or position of the United States Navy, the Department of Defense, or the United States government. This book is cleared for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
xx-12-1999	Special ("White Paper")	

4. TITLE AND SUBTITLE

Cyberterror: Prospects and Implications

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Nelson, Bill; Choi, Rodney; Iacobucci, Michael; Mitchell, Mark; Gagnon, Greg

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Naval Postgraduate School
Center for the Study of Terrorism and Irregular Warfare
Monterey, CA 93943

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 is unlimited.

13. SUPPLEMENTARY NOTES

The views expressed in this report are those of the authors and do not reflect the official policy or position of the United States Navy, the Department of Defense, or the United States government. Project supervisors: Dr. John Arquilla, Dr. David Tucker

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER (include area code)
U	U	U	UU	130	

Table of Contents

Foreword

There is a poignant moment, at the close of "His Final Bow," when Sherlock Holmes turns to Watson and says, "there is an east wind blowing... and a good many of us may wither before its blast." He was referring to the German threat, of course; but his comment was prescient, in that "the east" has bedeviled the 20th century. In addition to Germany, Japan, the old Soviet Union, and China have each posed significant security concerns. But, just as the "eastern threat" seems finally to have been taken well in hand, a new set of problems has emerged, emanating from rogue states, criminals and terrorists. They are capitalizing on a modern trend that witnesses the increasing destructive power of small groups, epitomized by new concerns about their acquisition of chemical, biological and nuclear weapons. And in addition to capabilities for mass destruction, the great dependence of most modern societies on advanced information technologies has also posed the prospect of vulnerability to mass disruption, principally from "cyberterror."

No less an authority on terrorism than Walter Laqueur has taken the position that attacks upon information, and information systems, can be as serious as attacks with some weapons of mass destruction. This view is implicitly accepted by the new Russian defense ministry, which reserves the right to respond to attacks on its infosphere "by any means."

This notion of the seriousness of the threat is echoed by American defense intellectuals and policymakers. From the recent reports of the President's Commission on Critical Infrastructure Protection, the National Research Council, and the Center for Strategic and International Studies at Georgetown University, one can see clearly the emerging sense of alarm at the onset of a new peril before whose onslaught many of us may "wither," as Sherlock Holmes would say.

All these assessments follow the same analytic approach, and share the same flaw. They catalog the dependency that comes with interconnectivity, and take as given the easy availability of the means of cyberattack. But all neglect the "demand side" of the problem. They don't examine why rogues and terrorists would want to cultivate capabilities for engaging in cyberterror.

This white paper begins the process of articulating the demand-side of cyberterror. In so doing, we provide some guidance for setting intelligence-gathering strategy. For, armed with useful hypotheses about the conditions under which terrorists might seek to acquire or develop their capabilities for mass disruption, the intelligence community may be able to provide at least some degree of early warning of this emerging

threat. And, based on the analysis that forms another part of our study, cyberterror is at best only an emerging threat, one far less dire than is suggested by others' assessments of this phenomenon.

Our view is not that cyberterror will fail to emerge as a serious threat. Rather, we see that the barriers to entry, for any capability beyond annoying hacks, are quite high; and that terrorists generally have neither the wherewithal nor the human capital needed to mount cyberterror operations on a meaningful level. Thus, because of the difficult technical path that must still be followed, cyberterror is not a threat. At least not yet, and not for a while.

Given this "breathing space," a period in which awareness of the potential vulnerability to cyberterror is keen, but the means of attack are not as yet properly honed, how should the defense intelligence community proceed? A two-track approach seems appropriate, forming a principal recommendation of this white paper. By this, we mean gathering intelligence on both the technical and the organizational developments taking place in terrorist groups.

A good indicator of a terrorist group's potential for cyberattack is likely to be the degree to which it is itself "informatized" (i.e., how much it uses the Net for communications, management, and intelligence gathering of its own). But as important are the group's own organizational dynamics. Is it a young or old group? Is it healthy or in decline? State-sponsored or not? Habituated to innovation or staid?

These are the sorts of broad organizational questions the answers to which will reveal much about the proclivity of any particular group to "go cyber." For, as the technical impediments to engaging in serious cyberterror decline in the coming years, the notion of understanding a group's "turn of mind" will become increasingly, and crucially, important.

Cyberterror is indeed coming. The anonymity afforded by means of attacking via the Net, the increasing economic damage that can be done by disruption, and the growing dependence of advanced militaries on interconnectivity all suggest that the infosphere is a fertile vineyard in which the terrorist may one day toil with good prospects for substantial rewards. This is all the more reason to think clearly about the technical requirements that must be met and the organizational incentives operative in groups that wish to take a path to cyberterror.

We believe that we have done some flinty-eyed analysis along these lines, and that we have contributed in two ways. First, we have exposed some of the hyperbole that accompanies the current literature on cyberterror. More importantly, though, in our view, we have provided a

conceptual framework for an intelligence-gathering strategy that will allow for more accurate assessments of what will certainly be a growing threat in the future.

John Arquilla
Monterey, CA

Summer 1999

Authors' Preface

Much has been made of the threat of cyberterrorism since the report of the Marsh Commission in 1997. However, current analyses have merely identified the plethora of vulnerabilities in automated information systems (computers) and assumed that terrorist organizations would be willing to exploit these vulnerabilities. They adopt a rudimentary strategic analysis and conclude that cyberterrorism is inevitable because it provides terrorists with a potentially strategic advantage over the United States.

We do not dispute the fact that our vulnerabilities are real and numerous. Further, we do not dispute that the consequences of exploitation are potentially severe, even strategically debilitating, if events unfolded in a manner described in some scenarios. However, based on our research, we also do not believe that terrorist organizations will soon possess the capabilities described in many of these scenarios.

According to many analyses, the necessary tools for exploiting vulnerabilities in the infrastructure are immediately available, easy to use, and proliferating at an alarming rate. Yet, the United States has not experienced any strategic attacks on critical infrastructure by terrorist organizations (or any other organization, for that matter). Even during the conflict in Kosovo, the most serious "attacks" consisted of vandalizing web pages and denial of service attacks on e-mail servers. Annoying, yes, but hardly a strategic threat to the United States or NATO. This suggests that these tools are still insufficient for the purpose of mass disruption, and that there are requirements for effective use that go beyond the mere possession of these tools and a desire to inflict damage.

Therefore, a key question we have asked is "Why haven't terrorist organizations taken advantage of this opportunity?" We believe that the costs of creating a capability sufficient to achieve terrorists' ultimate goals are much higher than the conventional wisdom indicates. Likewise, simply offsetting development costs is but one of several challenges that must be taken into account. Terrorist organizations will likely measure the benefits of pursuing cyberterrorism from the perspective of both internal and external incentives. Besides development costs, internal incentives must also include the individual and group psychological processes that heavily affect terrorist organizations. In terms of external interests, the costs of pursuing cyberterror may never be attractive as long as traditional terrorist methods remain viable.

We examined the issue of cyberterrorism from the perspective of an organization seeking to conduct a comprehensive assessment of its activities. Our assessment explores the costs, risks and benefits of adopting cyberterror,

either as a stand-alone operation or as an adjunct to traditional terrorist operations. We believe that this analysis fills a gap in the current literature on cyberterrorism. While the assessment is by no means comprehensive, it offers the intelligence community a much-needed starting point for better understanding the true potential of this threat.

Executive Summary

He who defends everything defends nothing

- Frederick the Great, 1749

There is every reason to believe that given the current world situation, terrorism in one form or another will continue to flourish. Most groups will continue to use traditional terrorist methods. These methods have been proven to provide the impact necessary to carry the terrorist message. For those groups that wish to expand their operational repertoire chemical, biological, radiological or nuclear weapons offer a dramatic option. The other option is cyberterror. The widespread vulnerabilities that many studies have previously identified make Cyberterrorism an attractive option.

To guide our thinking about cyberterror, we began by adopting the Department of Defense definition of terrorism. Based on that definition and the necessity that cyberterrorism must qualify as a subset of terrorism, we produced the following definition:

> Cyberterrorism is the calculated use of unlawful violence against digital property to intimidate or coerce governments or societies in the pursuit of goals that are political, religious or ideological.

We further recognized that cyberterror may come in many forms; and defined three levels of cyberterror capability:

> Simple-Unstructured: The capability to conduct basic hacks against individual systems using tools created by someone else. The organization possesses little target analysis, command and control or learning capability.
>
> Advanced-Structured: The capability to conduct more sophisticated attacks against multiple systems or networks and possibly, to modify or create basic hacking tools. The organization possesses an elementary target analysis, command and control and learning capability.
>
> Complex-Coordinated: The capability for coordinated attacks capable of causing mass-disruption against integrated, heterogeneous defenses (including cryptography). Ability to create sophisticated hacking tools. Highly capable target analysis, command and control, and organizational learning capability.

At the simple, low end, a terrorist group may use openly available tools to interfere with the computers of government response forces. At the complex, high-end, terrorists may seek to disrupt basic services in a large geographic area.

To determine "demand" for a cyberterror capability, we analyzed the goals, ideology and psychology of the types of terrorist groups, and the perceived utility of the three capability levels.

Of the five terrorist group types (religious, New Age, ethno-nationalist separatist, revolutionary, and far-right extremist), only the religious groups are likely to seek the most damaging capability level; as it is consistent with the indiscriminate application of violence that has distinguished much of their activity. The most immediate threat is found in the New Age or single-issue terrorist community (e.g. Animal Liberation Front). These groups are the most likely to accept disruption as a substitute for destruction. Both these groups and their primary targets are located in locales rich in information technology targets. These groups have, by far, the best match between desire, ideology and environment to support a near term advanced-structured attack threat.

Among the remaining ideological types, both the revolutionary and ethno-nationalist separatist (ENS) groups are likely to want an advanced-structured capability. For the revolutionary group, the advanced-structured level offers the necessary degree of control over side-effects. For the ENS group, this level provides sufficient impact to serve as an adjunct to its traditional terrorist acts.

In contrast, far-right extremists are not likely to seek anything more than a simple-unstructured capability. Cyberterror offers neither the intimacy nor the cathartic effects that are central to the psychology of far-right terror. The far-right groups have also made the greatest use of computer networks in support of their operations. Any widespread disruption is thus likely to affect their constituency as much as it does their enemies.

Turning our attention to those that likely already possess the technical wherewithal for sophisticated strikes, we see that hacker groups are psychologically and organizationally ill suited to mount such offensives. They tend to feature loose affiliations without the centralized direction necessary for sophisticated attacks on infrastructure targets. Perhaps more importantly, it is against their own self-interest to cause mass disruption to the information infrastructure. They have more reason to want The Net up than to take it down.

Any organization that commits to adopting more than simple-unstructured cyberterror faces a long, hard road. Today's information technology

professionals are in high demand and are well compensated. This reflects the difficulty of mastering information technology. The technical skills associated with the advanced-structured level include mastery of at least one operating system and one network protocol, as well as programming for both stand-alone and networked computers. At the complex level we add knowledge of industrial and control network protocols to the obvious expansion of the topics in the previous level. Closely tied to technical skill is an analytic ability. The cyberterror organization must be able to perform a detailed target analysis. Finally, the group must be able to plan and orchestrate the event to within very narrow tolerances.

Given these demands, a group starting from scratch can expect to reach the advanced structured level in no sooner than a year. More likely, it will take between two to four years. Groups seeking a complex-coordinated capability can anticipate expending at least an additional year. Realistically, though, the group should plan for six to ten years of effort from the time they first begin. The minimum figures only account for the academic, technical requirements. The predicted figures include time to develop experience in all three facets of the cyberterror capability. For groups that cannot wait this long, outsourcing or sponsorship may prove an attractive alternative.

Whether a group will pursue an internal or external sourcing method is tied closely to its organizational condition. Emerging groups, whose members may have already invested the necessary time and effort for the technical skills, are most likely to pursue a cyberterror capability internally. In contrast, declining organizations face a time imperative that demands external sourcing, probably through a sponsor. Splinter groups will also seek external support, though they may choose to find that support on the "open market." Stable groups have all options available to them. Their choice will be driven by circumstances peculiar to the individual group.

All of these factors combined indicate that pure cyberterrorism is a thing of the future. For the present, terrorists are much more likely to pursue cyberterror as an ancillary tool. However, as time and resources permit, groups of certain ideological types at particular growth stages will attempt to build on already existing cyberterror capabilities, constituting a "gradualist approach" to increasing their effectiveness.

Before this happens, the defense intelligence community should apply this framework to help identify the likely candidates for advanced cyberterror capability, and focus collection resources accordingly.

I. Introduction

> Our foes have extended the fields of battle – from physical space to cyberspace.
>
> - President Clinton, 22 May 1998

> If the new terrorism directs its energies toward information warfare, its destructive power will be exponentially greater than any it wielded in the past- greater even than it would be with biological and chemical weapons.
>
> - Walter Laqueur, "*Postmodern Terrorism*"

A. Background

As the world changes at an unprecedented pace, the likely nature of future conflict seems less clear. Although still relatively young, the Internet, which already claims 120 million users, continues to grow explosively. By 2005, an estimated 1 billion people, about one in every six humans, will be connected to the Internet. Americans, who today account for over 50% of all users, continue to see their banking activities, commerce, entertainment, and education migrate to the net. However, along with this increasing interconnectivity, America's critical infrastructures have been developing an information network dependency.[1]

Although natural phenomena (hurricanes, tornadoes, earthquakes, etc.), accidents, component and operator failure, can destroy or disrupt elements of the infrastructure, deliberate attacks could potentially cause even more significant harm, especially when used in conjunction with physical threats.[2]

---

[1] President's Commission on Critical Infrastructure Protection, *Critical Infrastructures: Protecting America's Foundations* (Washington, D.C.: GPO, 1997), pp. 3-4. Telecommunications, electrical power systems, gas and oil storage and transportation, banking and financial operations, air and rail systems, water supply systems, emergency services (medical, police, fire, and rescue), and continuity of government, are so vital that their incapacity or disruption could potentially have a debilitating impact on the defense and economic security of the United States. See also The White House, Office of the Science and Technology Advisor, *Cybernation: The American Infrastructure in the Information Age* (Washington, D.C.: GPO, 1996).

[2] However, the current ability of any actor to achieve widespread and persistent disruption that is severe enough to have strategic consequences is unknown. While many states are attempting to develop strategic information warfare capabilities, their level of development is difficult to determine. The actual consequences of such an action are still open to debate.

Attacks on critical infrastructure exist in two forms: physical (or kinetic) attacks against property and "cyber attacks" on the information systems that facilitate control of the infrastructure.[3]

The Department of Defense (DoD) provides a good illustration of this growing dependency.[4] It is an essential instrument and symbol of American power, and an adversary could exploit its reliance on information systems. Although DoD employs many safeguards to ensure the proper functioning of its communication systems, it may well be as vulnerable as the rest of American society.

> Defense has to protect a vast and complex information infrastructure: currently, it has over 2.1 million computers, 10,000 local networks, and 100 long-distance networks. Defense also critically depends on information technology--it uses computers to help design weapons, identify and track enemy targets, pay soldiers, mobilize reservists, and manage supplies. Indeed, its very warfighting capability is dependent on computer-based telecommunications networks and information systems.[5]

For the DoD, the Internet represents "a medium for less-sensitive national security communications, 95% of which depend on the public switch network."[6] A 1996 report by the General Accounting Office (GAO) found that DoD "computer systems are particularly susceptible to attack through connections on the Internet, which Defense uses to enhance communication and information sharing."[7] Although essential command and control systems are not connected to the Internet, numerous support functions, such as weapons systems research and development, logistics, and finance make use

---

[3] "Cyber attacks" include computer network attack through unauthorized access, viruses, Trojan horses, and other forms of malicious software and activity. For the purpose of this report, cyber attacks also include attacks with electromagnetic pulse or directed energy weapons.

[4] It is important to note that the vulnerabilities of DoD are not unique. A General Accounting Office (GAO) audit of 24 government agencies concluded that "significant information security weaknesses" existed in each agency. See General Accounting Office, *Serious Weaknesses Place Critical Federal Operations and Assets at Risk* (Washington D.C.: GAO, 1998), p. 5.

[5] General Accounting Office (GAO), *Computer Attacks at Department of Defense Pose Increasing Risks* (Washington, D.C.: GAO, 1996), p. 3. Although the oft quoted numbers of 250,000 "attacks" a year has been discredited because of the expansive definition of an attack, the essential conclusions of the report remain unchallenged.

[6] P. Constantini, "Virtual Armies Clash by Net" *LEXUS/NEXIS* Inter Press Service, 4 June 1996.

[7] GAO, *Computer Attacks,* p. 3.

of the Internet.[8] Further, the Internet is only a portion of the information infrastructure. Defense installations are still subject to the disruption of electrical power and other communications networks, such as the Defense Information Systems Network (DISN) and the Global Command and Control System (GCCS).[9] Disrupting these systems during a crisis could seriously impair the ability of the United States to deploy or sustain its forces.

B. Purpose

This study will provide a framework for analyzing the group dynamics and environmental factors that may lead terrorist organizations to integrate cyberterror into their current operations, or drive hacker activity towards terrorism. The framework can assist the Intelligence Community (IC) in understanding and evaluating the potential threat from cyberterrorism.

C. Relevance

The majority of literature dealing with cyberterrorism has focused principally on the *vulnerabilities* of critical infrastructures. [10] While the studies have well documented the potential vulnerabilities, the studies have consistently been alarmist in nature regarding the threat to these infrastructures.[11] Prior studies have failed to address in any detail the motivation, intent, resources, risks, and benefits for non-state actors attempting to exploit these vulnerabilities. Our

---

[8] GAO, *Computer Attacks,* p. 10. DoD is attempting to develop an independent network, the Global Network Information Enterprise project (GNIE) based on Internet protocols. It would completely move its unclassified networks off the Internet. John Schwartz, "Online Security Is Pentagon's Latest Battle" *Washington Post,* 2 June 1999, p. A-2. Additionally, Assistant Secretary of Defense John Hamre ordered the removal of sensitive information from all DoD Internet sites in a Sept. 25, 1998 memo. This was a result of increased awareness of the vulnerabilities created by posting information on the Internet.

[9] DISN is a "composite of certain DoD information systems networks under the management control and...operational direction of DISA [the Defense Systems Information Agency]." GCCS "incorporates the core planning and assessment tools required by the combatant commanders and their subordinate joint force commanders." Joint Chiefs of Staff (JCS), *Joint Pub 6-0: Doctrine for Command Control, Communications, and Computer (C4) Systems Support to Joint Operations* (Washington D.C.: Department of Defense, 1995), pp. VI-1 – VI-4. Although these systems are more secure than other networks, they are still vulnerable to disruption from loss of electrical power or the physical destruction of network nodes or segments.

[10]The President's Commission on Critical Infrastructure Protection (PCCIP), the National Security Telecommunications Advisory Committee (NSTAC), the General Accounting Office and numerous other organizations have analyzed and identified infrastructure vulnerabilities.

[11]Vulnerability is not synonymous with threat. A vulnerability is a weakness in a system that may be exploited. A threat requires an actor with the motivation, resources, and intent to exploit a vulnerability.

study differs from previous studies by addressing the motivations, organizational implications, and technical barriers to entry faced by an organization wanting to conduct attacks on critical infrastructures. We believe our method, which weighs both the costs and benefits of cyberterror, can provide a more accurate forecast of cyberterror activity, both in a support role to traditional terrorism and as a possible new, stand-alone terrorist tactic.

D. Methodology/Design

This study uses an inductive approach to formulate a general framework. Based on previously published analyses of the motivation, intent, capabilities and resources of traditional terrorist organizations, we develop a framework to analyze the prospects for cyberterrorism. This framework is designed to identify useful insights regarding the development and use of cyberterror, from the perspective of a terrorist organization.

E. Limitations

This study addresses only transnational terrorist organizations; it does not consider domestic terrorist organizations in the United States. Further, we do not specifically address the "insider threat" to information systems. Nor do we provide a comprehensive group-by-group analysis. Rather, we establish a framework and make general assessments based on information and intelligence regarding terrorist organizations and, their ideologies. The diversity of terrorist motivations and the opaque nature of their organizations make it extremely difficult to predict specific terrorist behavior. The nearly endless supply of "soft targets" also complicates any predictive efforts. This problem is particularly acute when addressing "terrorism" as a whole rather than specific terrorist groups. Nonetheless, performing this broadly based analysis is a necessary first step in understanding and countering an emerging threat.

This report does not provide any additional analysis of vulnerabilities of critical infrastructures. The vulnerabilities of critical infrastructures have been widely examined by a multitude of individuals and organizations. Our analysis is based on contemporary circumstances and does not purport to address future scenarios. However, the framework developed should be applicable across the range of possible futures.

F. Structure of the Study

The study is divided into five major chapters and addresses a number of diverse, but interrelated, questions. Chapter II examines existing definitions of terrorism and establishes definitions of cyberterror, differentiating between

cyberterror attacks and cyberterror support. Additionally, this chapter defines three levels of cyberterror capability to guide a more detailed analysis of terrorist motivations and resources. Chapter III identifies significant trends affecting the viability and likelihood of terrorism in general. It also examines the specific opportunities for and threats to terrorist organizations wishing to pursue cyberterrorism.

Chapter IV examines the utility of cyberterrorism to specific types of terrorist organizations, independent of resource constraints. The organizational analysis applied in this chapter considers ideology, group psychology, and internal organizational requirements. Chapter V examines the necessary skills and resources needed to reach any of the three levels of cyberterror. Chapter VI addresses the barriers to entry in conjunction with the various implementation options for groups that decide to pursue cyberterrorism. The costs and benefits of the implementation options and the incentives for state sponsorship are considered. The final chapter presents conclusions and recommendations for future research.

G. Findings

Advanced-structured and complex-coordinated cyberterrorism will likely be pursued by only a few terrorist organizations. Of these, the most dangerous eventuality will likely come from a newly-formed religious group. However, this is a long-term threat. More likely, near-term threats may be posed by stable, new age terrorist groups. We recognize also that several less dramatic threats at the simple and advanced-structured levels also merit further consideration by the intelligence community.

II. Definitions

> Above the gates of hell is the warning that all that enter should abandon hope. Less dire but to the same effect is the warning given to those who try to define terrorism. [12]

This chapter attempts to relate the concept of cyberterror to existing notions of terrorism, terrorist activity, and terrorist acts. A comparison of existing definitions of terrorism provides the basis for a definition of cyberterrorism. Special attention is paid to property destruction, in an effort to illuminate how property destruction, which often requires little violence, and seldom produces fear, has come to be accepted as a true form of terrorism. Despite claims to the contrary, cyberterrorism has only a limited ability to produce the violent effects associated with traditional terrorist acts.[13] Therefore, to consider malicious activity in cyberspace "terrorism," it is necessary to extend existing definitions of terrorism to include the destruction of digital[14] property. The acceptance of property destruction as terrorism allows this malicious activity, when combined with the necessary motivations, to be defined as cyberterror. Finally, the chapter concludes with a description of threat capabilities, categorized in three levels.

A. Terrorism

In the search for a clear definition of terrorism, about the only constant is that people continue to disagree. During our research, we reviewed academic,[15] State Department (Title 22 U.S. Code, Section 2656f(d)), the Federal Bureau of Investigation, and the Department of Defense (Joint Publication 1-02)

---

[12] David Tucker, *Skirmishes at the Edge of an Empire: The United States and International Terrorism* (Westport, CT: Praeger Publishers, 1997), p. 51.

[13] See Barry C. Collin, "The Future of Cyberterrorism: Where Physical and Virtual Worlds Converge" *Crime & Justice International* 13.2 (March 1997). Available at http://www.ascp.uic.edu/oicj/pubs/cjintl/1302/130214.shtml; Walter Laqueur, "Postmodern Terrorism" *Foreign Affairs* 75.5 (Sep/Oct 1996): 24-36; and The Center for Strategic and International Studies (CSIS) Global Organized Crime Project, *Cybercrime...Cyberterrorism...Cyberwarfare... Averting an Electronic Waterloo*, ed. Frank J. Cillufo, Bruce D. Berkowitz, and Stephanie Lanz (Washington, D.C.: CSIS, 1998).

[14] In using the term "digital" we recognize that electronic information may be at times represented in analog form. For clarity we include both forms when using the term digital.

[15] Thomas Perry Thornton, "Terror as a Weapon of Political Agitation," *Internal War: Problems and Approaches.* ed. Harrry Eckstien. (New York: Free Press of Glencoe, 1964), p. 73. and E.F. Mickolus, *Transnational Terrorism: A Chronology of Events, 1968-1979* (London: Aldwych Press, 1980), p. XIII-XIV as quoted in Alex P. Schmid, *Political Terrorism* (New Brunswick: Transaction Books, 1983), p. 73. and R. Clutterbuck, *Guerrillas and Terrorists* (London: Faber and Faber, 1997), pp. 11 & 21 as quoted in Schmid.

definitions for terrorism. The discontinuity noted in academic definitions continues to be present in various U.S. Government (USG) agencies' definitions. For the State Department:

> The term "terrorism" means the premeditated, politically motivated violence perpetrated against noncombatant (1) targets by subnational groups or clandestine agents, usually intended to influence an audience. ...Noncombatant – to include, in addition to civilians, military personnel who at the time of the incident are unarmed and/or not on duty. [16]

The State Department's definition of terrorism is interesting because it does not specifically include actions against "property." However, the incident database reflected throughout the State Department's Patterns of Global Terrorism, (1998) does reflect attacks against U.S. commercial property such as oil pipelines in Colombia. In fact,

> About 40 percent of the (international) attacks in 1998 – 111 - were directed against US targets. The majority of these - 77 - were bombings of a multinational oil pipeline in Colombia, which terrorists regard as a US target.[17]

Drawing from this, we also note that the USG Title 22 definition, in practice, clearly includes destruction of property as terrorism when the other conditions for terrorism are satisfied (premeditated, politically motivated, etc.).

Unlike the State Department definition, the FBI's definition explicitly includes acts against property.

> The unlawful use of force or violence against persons or property to intimidate or coerce a Government, the civilian population, or any segment thereof, in furtherance of political or social objectives.[18]

As noted in the Department of Defense (DoD) regulation O-2000.12-H, "...it is important to remember that the DoD definition [logically] subsumes both definitions used by the FBI and the DoS [Department of State]."[19] In an effort to be inclusive, the definition of terrorism used in this study will remain

---

[16] United States Department of State, *Patterns of Global Terrorism: 1997*, p. 4.

[17] United States Department of State, *Patterns of Global Terrorism: 1998* (p. 1, section "The Year in Review"). http:www.state.gov/www/global/terrorism/1998Report/review.html

[18] DoD O-2000.12-H, p. 2-1.

[19] DoD O-2000.12-H, p. 2-1.

consistent with the broader DoD definition as detailed in Joint Publication 1-02 and the DoD regulation O-2000.12-H.

> Terrorism – the calculated use of unlawful violence or threat of unlawful violence to inculcate fear: intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological. [20]

In the State Department and FBI definitions, the use of "violence" as it applies to property damage is generally recognized in the form of property destruction. The DoD regulation cited above does include "malicious property destruction"[21] as a type of terrorist attack. The regulation also begins to address destruction at the binary code level and specifically refers to it under the use of special weapons:

> Use of sophisticated computer viruses introduced into computer-controlled systems for banking, information, communications, life support, and manufacturing could result in massive disruption of highly organized, technological societies. Depending on the scope, magnitude, and intensity of such disruptions, the populations of affected societies could demand governmental concessions to those responsible for unleashing viruses. Such a chain of events would be consistent with contemporary definitions of terrorist acts.[22]

As outlined above, the DoD institutional definition of terrorism includes not only property destruction, but also begins to expand terrorism into the realm of cyberspace. The following section provides a framework for understanding the phenomenon of terrorism as applied to cyberspace and information systems.

B. Cyberterror

> Cyberterrorism is the unlawful destruction or disruption of digital property to intimidate or coerce governments or societies in the pursuit of goals that are political, religious or ideological.

As a subset of terrorism, cyberterror involves using information as a weapon, method, or target, to achieve terrorist goals. Cyberterror exists in and beyond cyberspace and includes physical destruction of any device, system of

---

[20] DoD O-2000.12-H, p. 2-1.

[21] DoD O-2000.12-H, p. 2-7.

[22] DoD O-2000.12-H, p. 2-10.

devices, or process with an information component. At the lowest common denominator, an information component can be understood to represent binary code. Acts taken to disrupt, deny service, destroy, and corrupt binary code are thus acts of cyberterror.

A characteristic of cyberterror is its ability to leverage inexpensive means to gain disproportionate effects through destruction, denial, deceit, corruption, exploitation, and disruption. Cyberterror can increase the destructiveness, or disruptiveness, of the act by enabling greater target coverage, effect, and efficiency. Cyberterror may augment or support traditional terrorism, or be employed as a distinct form of action in its own right.

C. Cyberterror Support

> Cyberterror support is the unlawful use of information systems by terrorists which is not intended, by itself, to have a coercive effect on a target audience. Cyberterror support augments or enhances other terrorist acts.

Like terrorist acts (bombings, assassinations, etc.) and terrorist activity (financial and logistical support), cyberterror can also be classified as either acts or activities.[23] For example, in order to accomplish a terrorist bombing, various terrorist activities are necessary to support the operation. Such activities include, but are not limited to, intelligence collection, communications, logistics, and supply requirements..

The intended outcome of the terrorist use of information technology determines whether a given incident qualifies as an attack or support. Attacks are events whose outcome is intended to "intimidate or coerce" in the direct pursuit of the attacking group's goals. An incident of cyberterror support is intended to augment or enhance some other act (or threatened act) of terrorism. The supported act may be traditional terrorism or cyberterrorism.

Terrorist use of information technology in their support activities does not qualify as cyberterrorism. Our definition does not include the otherwise legal use of information technology by terrorist organizations.[24] While such use may improve the distribution of the terrorist message or enhance the efficiency of

---

[23] For clarity and continuity throughout this study, we substitute act and activity for attack and support, respectively. This applies to both traditional terrorism and cyberterror. We choose to use the military forms of expression.

[24] Note that this definition excludes activities such as electronic mail between group members and propaganda dissemination. The definition also excludes the legal collection of information posted to the worldwide web. While this can be a powerful tool for terrorists we see this as equivalent to library research which would not be classified as terrorism.

terrorist groups, such activities cannot be construed as cyberterrorism if we are to remain precise about our definitions.

We attempt to clarify the distinction between cyberterror attacks and support by examining them in terms of the concepts of confidentiality, integrity, and availability. A breach of confidentiality occurs if an unauthorized user gains access to information. A breach of confidentiality is an act of cyberterror support. The classic example of a confidentiality violation is acquiring another user's password. Violations of confidentiality are essentially passive. It is only when the terrorist group threatens (or implies the threat of) some action with the stolen information that they cross into cyberterror attacks.

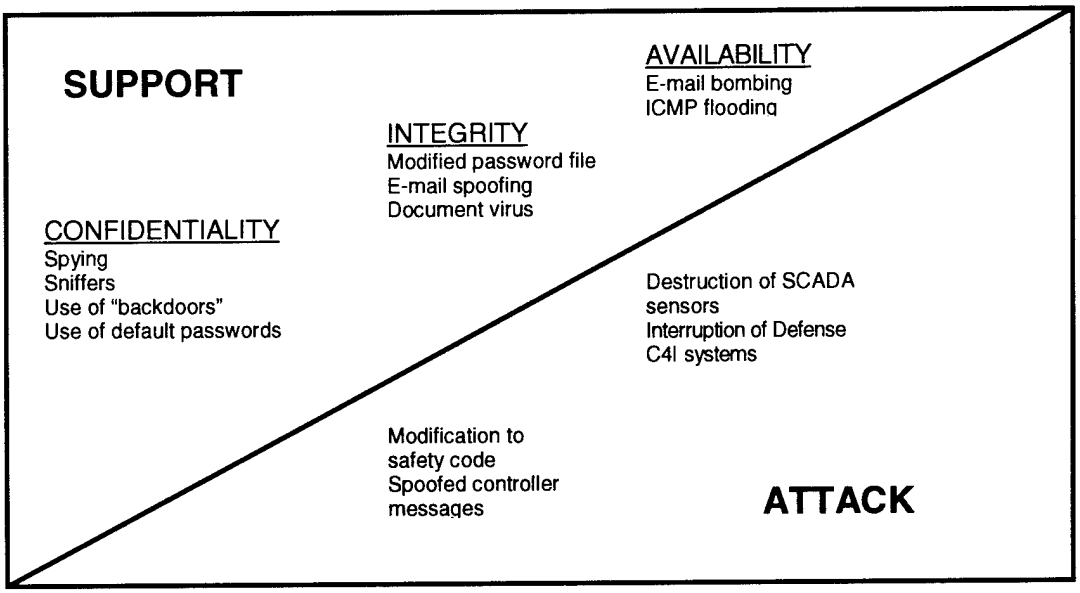


Figure 2-1: Comparison of Cyberterror Attack and Support

Violations of the integrity of an information system occur when the information the system uses (either program instructions or data) is modified. This includes both covert changes to and outright destruction of data.[25] These modifications can occur while the information resides within a component or when the information is in transit between components. Incidents that violate integrity may be categorized as either attacks or support. Surreptitious modification of a user account to allow an attacker access to a key system, without the threat of action, has no coercive effects.[26] On the other hand, the publicized modification of train routing software intended to produce a collision will intimidate a target audience.

[25] Destruction includes anything from a bomb, to an EMP device, or simply "erasing" the data.

[26] It is the threat of what the terrorist may do with this account that intimidates the populace.

Availability refers to the ability of legitimate users to access information and information resources. Violations of availability are generally referred to as "denial of service attacks." However, our definition allows violations of availability to be either attacks or support. Losses of service can occur as unintended side effects.[27] This can hardly be intended to "coerce or intimidate." Similarly, a denial of service attack against a computerized security system that prevents the detection of physical access to an embassy is an enhancement to an attack and thus cyberterror support. In contrast, denial of air traffic control services would constitute an attack, because of the potentially dire consequences.

Although all cyberterror acts imply a violation of confidentiality, integrity or availability, the reverse is not true. Other criminal acts perpetrated through or against information systems for non-terrorist purposes are not cyberterrorism. Terrorism represents the intersection of violent criminal activity and political activity. The political nature of terrorism is what separates it from other criminal activity motivated by financial gain or personal animosity. In general, espionage and criminal activity do not constitute terrorism, and should not be considered part of cyberterrorism. Therefore, these types of criminal activities are excluded from our definition, and from this study.

The distinction between common criminal activity and cyberterrorism involves a substantial gray area – cyberspace activities by terrorist groups principally intended to provide financial support for other operations. This is a real possibility, especially for groups that lack a sponsor or profit-producing front organization. Additionally, other authors have argued that the definition of terrorism must be expanded to include economic motivations[28] and activities by transnational criminal organizations (TCOs) but that analysis of is beyond the scope of this study.

Although the use of information-networks to support criminal activity continues to grow, such as Internet based money laundering, this use is not analyzed herein. For the drug cartel, a type of TCO, profit is the ultimate motivating factor. For terrorist organizations and state institutions, cyberterror activities are motivated by political aims. With regard to cyberterror, it is necessary to remember that the act must first be a form of terrorism before the act can be classified as cyberterror. This distinction will allow us to segregate cyber crime from cyberterror.

---

[27] For instance, some network scanning software can cause some components to become unstable and fail.

[28] Roger Medd and Frank Goldstein, "International Terrorism on the Eve of a New Millenium," *Studies in Conflict and Terrorism* 20.3 (Jul-Sep 1997): pp. 281-316.

Recognizing that new definitions can be difficult to conceptualize, we provide the following example to help clarify the meaning of cyberterror:

> Cyberterror Attack Scenario:
>
> A plane crash is caused, not by a bomb, but through a pulse device. The pulse device was transported on board with a passenger. The intent of the pulse is to disrupt and permanently corrupt the information system components within the aircraft. One disrupted control process affected by the pulse was the landing gear control component. Without the landing gear in the correct position, among other problems, the plane attempts to land safely but is unsuccessful.

If, in this example, a bomb were substituted for the pulse device, and the other conditions for a terrorist act were met (intent, etc), then there would be little debate as to the nature of the violence – it is terrorism. From this extreme example, the argument is not difficult to make. Examining examples where individuals are not placed in life threatening (fear producing) situations, though, begins to complicate the definition. Nevertheless, we argue that the same criteria applied to traditional terrorism should also be applied to cyberterror. Once again we highlight the Colombian terrorist bombings of oil pipelines as an example where terror, in the life threatening form, fails to develop; but where the incident is indeed categorized as a terrorist act. We do not dispute the legitimacy of the bombing act in this case. Furthermore, we employ the same logic when we propose that a cyberterror attack be accepted as a form of terrorism.

D. Levels of Cyberterror – Defining Capabilities

Not all threats are "created equal." Any analysis of threats must discern the varying capabilities of potential adversaries. To date, other studies such as those published by the PCCIP, the CSIS, the National Research Council and NSTAC have all failed to do this. We identify three distinct capability levels, which pose correspondingly distinct threats. Chapter V of this study will define in detail the component skills, and the barriers to achieving those skills, for each level of cyberterror capability. As we will argue, achieving the most robust capability entails significant challenges for existing terrorist organizations – not only organizational restructuring, but possibly a change in culture – all of which may decrease the likelihood that this capability level will be realized.

The characteristics of the three levels (simple-unstructured, advanced-structured, complex-coordinated) help quantify the different skills and resources required for a proposed capability. The levels are defined in terms

of target scope, target analysis, degree of control over intended effects,[29] potential utility, and target selection methodology.

> Simple-Unstructured: The capability to conduct basic hacks against individual systems using tools created by someone else. The organization possesses little target analysis, command and control or learning capability.

Simple-unstructured cyberterror includes direct probing,[30] and probing with malicious secondary source software. Simple-unstructured cyberterror is a small-scale capability to conduct basic hacks against individual systems using basic computer skills and openly available malicious software from a secondary source (such as a hacker web page). This level of cyberterror is also characterized as simple due to the lack of target analysis and the method of target selection. Targets are selected primarily based on available tools and poor security procedures, not because they have are tactically or strategically significant. The organization lacks the resources and skills to create tools for attacking selected targets; they are dependent on the resources provided by the hacker community.

Organizations with a simple-unstructured capability may exhibit low confidence in the organization's ability to integrate cyberterror into its existing and future operations because the organization is dependent on secondary source hacker software. Electronic mail "bombing" attacks[31] and some web page hacking can be characterized as simple-unstructured attacks. The potential strategic utility of these attacks is low due to the short duration, and limited scope and consequences.

---

[29] Degree of control over intended effects – describes whether the consequences of the cyberterror are manageable by the originator.

[30] Direct probing – attempts to access via normal though not intended channels (default accounts or compromised user id and password pairs).

[31] Flooding a site with unwanted mail to cause its servers to fail.

Cyberterror level	Target Scope	Target Analysis	Effects Control	Potential Utility	Target Selection Method
Simple - Unstructured	Single system or network	None	Unfocused	Propaganda/Harass-ment, Recruiting	Existing tools => target
Advanced - Structured	Multiple systems or networks	Elementary	Focused	Tactical Strikes (for demonstration purposes or in support of conventional operations)	Target => find or modify existing tools
Complex - Coordinated	Multiple networks	Detailed	Scalable or controlled	Strategic strikes for coercive or defensive objectives	Target => develop necessary tools or optimize existing tool(s)

Table 2-1: Levels of Cyberterror

Advanced-Structured: The capability to conduct more sophisticated attacks against multiple systems or networks and possibly, to modify or create basic hacking tools. The organization possesses an elementary target analysis capability and command and control structure for sequential attacks from a single location. Some learning ability - can assimilate some new technologies and train personnel.

Cyberterror activity at the advanced-structured level is more focused in its effects than simple-unstructured cyberterror. At the advanced-structured level, an elementary target analysis is conducted to determine the targeted system's configuration and system parameters. This level provides a degree of assurance regarding the immediate effects of the attack on the targeted system but the organization would be unlikely to understand secondary effects. At this level, the organization would possess some programming skills and a sufficient understanding of the targeted system to create basic hacking tools or modify existing ones. The organization may also possess knowledge of a variety of information systems. An organization with the ability to operate at the advanced-structured level may be able to integrate cyberterror and provide operational support for conventional terrorist operations.

Organizations with an advanced-structured capability will require an internal learning mechanism to understand and assimilate new technology and train personnel. Recognizing that this is an organizational imperative is critical; the internal training mechanism represents a turning point in an organization's cyberterror capability. The organization can grow from a cyber opportunity taker, created by the environment, to an opportunity maker with the ability to influence the cyber environment. Although the turning point for pursuing more advanced capabilities resides at this level, the disruption that can be achieved at the advanced-structured level is still limited, due to a lack of understanding in multi-system or networked targets.

Complex-Coordinated: The capability for coordinated attacks capable of causing mass-disruption. Ability to analyze vulnerabilities, penetrate integrated, heterogeneous defenses (including cryptography) and create attack tools. Strong ability to conduct target analysis and high confidence in results. Strong command and control structure capable of employing multiple, simultaneous attacks from different locations. Strong organizational learning capacity – can keep up with latest technology, train personnel, diffuse knowledge throughout the organization, make necessary doctrinal and organizational changes to enhance capabilities.

In comparison to lower levels, only a small percentage of individuals are capable of executing the tasks categorized as complex-coordinated cyberterror. At this level, the terrorist group understands various software,

hardware, and firmware characteristics of the targeted systems. Further, they possess sufficient intelligence gathering and analysis capabilities to enable them to predict the secondary and tertiary effects of their attacks. They may also possess the capability to defeat some encryption measures and take advantage of covert channels. This detailed understanding of networks and computer science coupled with detailed target analysis, with respect to the configuration and status of the targeted network, creates the ability for the terrorist to manage the spread of effects from the cyberterror activity. This capability includes the ability to develop malicious software, and is characterized by direct penetration[32] and subversion of security mechanisms.[33] An organization at this level would have a high degree of assurance of achieving the desired effects. It would also possess a strong organizational learning capacity, and exhibit strong command and control. The organization's ability to assimilate and understand new technology will drive the organization's capability. To assimilate the technology, the organization must train its personnel and diffuse knowledge throughout the organization.

At the complex-coordinated level, the utility of cyberterror progresses along two avenues. First, fully integrated cyberterror support enhances conventional terrorist acts and activity. However, it is also at this level that cyberterror can operate in a sufficient manner to be effective in a stand-alone mode. Only at this level can cyberterror be considered a possible threat to multi-networked infrastructures, or even single-networked infrastructures with numerous types and brands of hardware, each with its own proprietary programming code. Groups at both the simple-unstructured and advanced-structured levels would lack the organizational expertise to acquire, analyze, and understand the information requirements for system-wide attacks.

[32] Direct penetration - bypassing intended security policies to create or take advantage of security holes.

[33] Subversion of security mechanisms – covert and methodical undermining of controls.

E. Summary

The following definitions set the conditions for the remainder of our study:

- Cyberterrorism is the unlawful destruction or disruption of digital property to intimidate or coerce governments or societies in the pursuit of goals that are political, religious or ideological.
- Cyberterror support is the unlawful use of information systems by terrorists which is not intended, by itself, to have a coercive effect on a target audience. Cyberterror support augments or enhances other terrorist acts.
- Simple-Unstructured: The capability to conduct basic hacks against individual systems using tools created by someone else. The organization possesses little target analysis, command and control or learning capability.
- Advanced-Structured: The capability to conduct more sophisticated attacks against multiple systems or networks and possibly, to modify or create basic hacking tools. The organization possesses an elementary target analysis capability and command and control structure for sequential attacks from a single location. Some learning ability - can assimilate some new technologies and train personnel.
- Complex-Coordinated: The capability for coordinated attacks capable of causing mass-disruption. Ability to analyze vulnerabilities, penetrate complex defenses (including cryptography) and create attack tools. Strong ability to conduct target analysis and high confidence in results. Strong command and control structure capable of employing multiple, simultaneous attacks from different locations. Strong organizational learning capacity – can keep up with latest technology, train personnel, diffuse knowledge throughout the organization, make necessary doctrinal and organizational changes to enhance capabilities.

With these definitions, and an understanding of the distinctions between cyberterror attacks and support activities, we are now able to address the range of factors that will influence an organization's desire to pursue cyberterrorism.

III. The Environment - Opportunities and Threats

A. Introduction

This chapter examines the current global operating environment. The fundamental question addressed in this chapter is whether this environment presents an opportunity for the use of cyberterrorism. It begins with a brief overview of the factors affecting the perceived utility of terrorism, and then gives a more detailed examination of the specific opportunities for and threats to those organizations that may pursue cyberterror. The macro-environmental factors indicate a continuing utility for traditional terrorism as a form of political violence. This, combined with information-age developments, will likely create localized environments conducive to cyberterrorism as well. However, a brief survey of significant indicators related to cyberterrorism reveals a heterogeneous growth of information infrastructure and technology utilization which may limit the "supply side" for cyberterror. This said, cyberterror will certainly be a growing threat in the future. It is only the rate of growth that is in question.

B. Global Factors Influencing Terrorism

- The dissolution of the Soviet Union and the end of the Cold War have created instability in many countries, and fostered the growth of regional powers.

- The dominant role of the United States in world affairs (politically, culturally, and economically) and its numerous interventions may engender resentment and provide rationales for some terrorist organizations.

- The conventional military power of the United States may drive adversaries to consider asymmetric approaches to confronting the United States.

- Ethno-nationalist separatists (ENS) are clamoring for independence and autonomy in dozens of states.

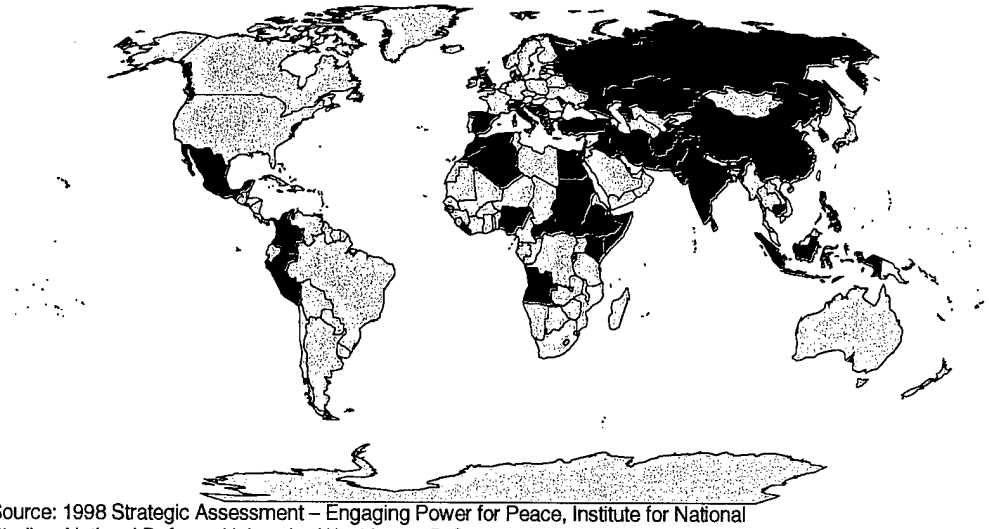
- Non-state actors form alliances unconstrained by geographic boundaries.

- The diffusion of technical knowledge concerning CBRN may allow terrorist organizations greater access to these weapons.

- BOTTOM LINE: Terrorism will persist and the United States will remain a target.

A variety of political and socioeconomic factors affect the continuing utility of terrorism. The most significant factors are the changing world security environment; the growth of non-state actors; the proliferation of chemical, biological, radiological, and nuclear weapons; and the growth of information-age societies.

The demise of the bipolar security environment has resulted in greater global uncertainty. Ethnic tensions suppressed by now defunct totalitarian regimes are reemerging, with demands for the right of self-determination. Long-standing ethnic conflicts threaten to break struggling states into smaller units by displacing allegiances from the state to the ethnic group.[34] Figure 3-1 provides a perspective on the pervasiveness of ethnic conflict. The darkened (red) areas represent areas of current or potential conflict, a large number of which are ethnically motivated. These quests for autonomy will continue to generate politically motivated violence.



Source: 1998 Strategic Assessment – Engaging Power for Peace, Institute for National Studies, National Defense University, Washington D.C.

Figure 3-1: Current or Potential Conflicts

As the sole superpower, the United States has assumed a unique role in international relations. Because of this role and a policy of engagement, the military might and force projection capabilities of the United States have been

[34] D. L. Horowitz, *Ethnic Groups in Conflict* (Los Angeles: University of California Press, 1985), pp. 4-6.

called upon frequently to intervene in crises around the globe. These interventions have served to highlight the superiority of our conventional forces and may drive future adversaries to consider asymmetric responses. Further, as the United States has responded to these crises in order to protect its security interests, it has undoubtedly engendered resentment. The aggrieved parties, unable to confront the United States with conventional forces, may resort to terrorist acts as revenge for these interventions.[35]

The international nation-state system will be challenged by the continued growth of non-state actors. Sub-state actors such as transnational criminal organizations (TCOs), multinational corporations (MNCs), and non-governmental organizations (NGOs) can create alliances that are not constrained by state boundaries. In economic matters, some MNCs have grown to such proportions that their annual revenues dwarf the budgets of most nation-states.[36] Some authors predict that these non-state actors will increase their power at the expense of the state.[37] In Mexico, the Zapatistas leveraged the possibility of disrupting growth by creating unfavorable conditions for foreign investment.[38]

---

[35] Ivan Elan, "Does U.S. Intervention Overseas Breed Terrorism?" Cato Institute Foreign Policy Briefing #50, 17 Dec. 1998.

[36] Extrapolating from the *Global 500 List* (see: http://cgi.pathfinder.com/cgi-bin/fortune/global500) maintained by Fortune Magazine, Mitsubishi's 1996 total revenues of 184,365 million US$ would place Mitsubishi 24th, just below Turkey, on the World Bank's 1999 World Development Indicators – Total GDP 1997 Listing. Just below Mitsubishi would be Mitsu (25th), another Japanese trading company, which would be followed on the list by Hong Kong, Denmark, Thailand, Norway, and Saudi Arabia. For a complete listing of Total GNP by country for 1997 see: http://www.worldbank.org/data/databytopic.

[37] Phil Williams, "Transnational Criminal Organizations and International Security," *In Athena's Camp,* ed. John Arquilla and David Ronfeldt (Santa Monica, CA: RAND, 1997), p. 329. "...it is clear that TCOs pose threats to security at three levels: the individual, the state and the international system of states." Also see pp. 332-333.

[38] Armando Martinez and David Ronfeldt "A Comment on the Zapatista 'Netwar'," *In Athena's Camp,* ed. John Arquilla and David Ronfeldt (Santa Monica, CA: RAND, 1997), pp. 380-382. The transnational criminal organization's lack of subservience to the state and the EZLN's use of propaganda to rile media attention and alarm foreign investors against investing in Mexico's economy show the growing power of the non-state actors.

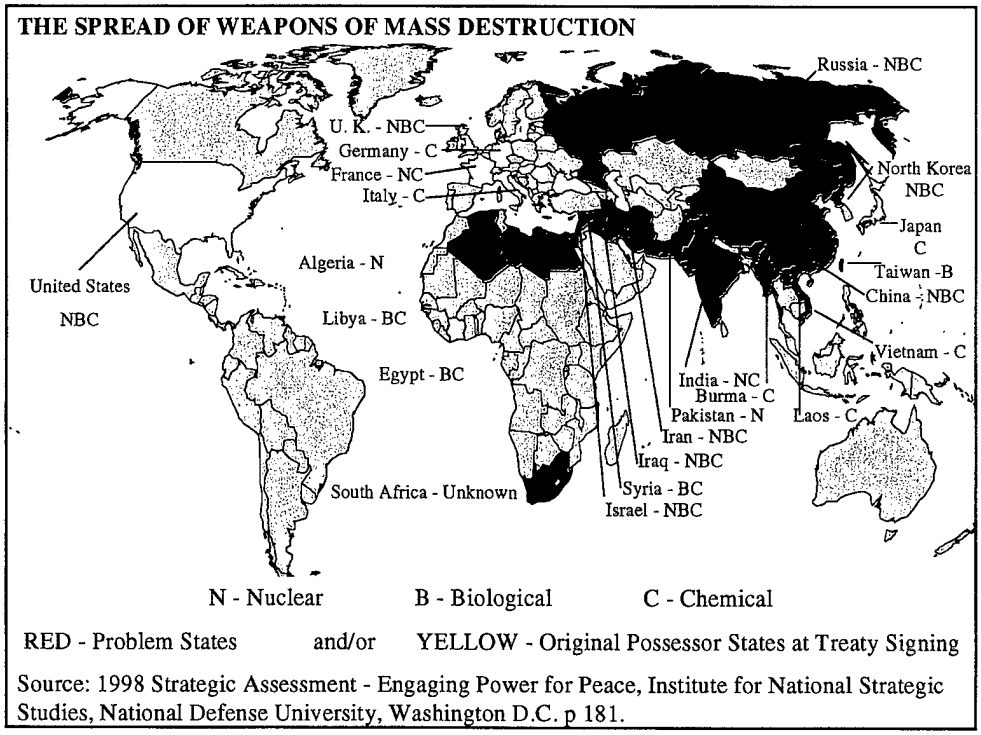


Figure 3-2: The Spread of Weapons of Mass Destruction

WEAPON	GOVERNING TREATY	POSSESSOR STATES AT TREATY SIGNING DATES	PROBLEM STATES
Nuclear (N)	Nonproliferation Treaty, 1970	US, UK, France, China, Soviet Union	Israel, India, and Pakistan. Active proliferators include Iran, Iraq, Algeria, and North Korea
Biological (B)	Biological Weapons Convention, 1975	US, UK, Soviet Union, and China	Iran, Iraq, Libya, Syria, Israel, Egypt, Taiwan, Vietnam, North Korea, and Laos
Chemical (C)	Geneva Protocol, 1925	US, UK, France, Soviet Union, Germany, Japan, and Italy	Egypt, Iran, Iraq, Israel, Libya, Syria, North Korea, Burma, Vietnam, China, and Russia

Table 3-1: CBRN Proliferation

The proliferation of Chemical, Biological, Radiological, and Nuclear (CBRN) weapons provides a potential strategic alternative to cyberterrorism. Although the pursuit of both capabilities is possible, most terrorist organizations do not have the resources to do so. Despite the obstacles and risks of pursuing

these weapons, they may still appeal to certain terrorist organizations.[39] Although no known terrorist group has succeeded in acquiring nuclear weapons, the potential cannot be summarily dismissed.[40] Similarly, with the notable exception of the Tokyo subway attack by Aum Shinrikyo, no terrorist organization has successfully used chemical or biological weapons on a large scale.[41] Again though, the possibility cannot be ruled out. Attempts to forecast proliferation are difficult at best, but certain trends seem obvious. For example, CBRN knowledge and materials will diffuse beyond those who possess such capabilities today.

As societies transition to the information age, terrorism will see its operating environment change as well; i.e. government, business, and the media will all be influenced. Because terrorism takes place on a global scale, any analysis of terrorism should include an assessment of both the global environment as well as the varying multiple microenvironments. For this study, analyzing both the macro- and microenvironment is critical.

The survey of the four variables affecting the future of terrorism yield the following results:

- A security environment where terrorism continues its utility as a form of political violence;
- More, not fewer, asymmetrical options available for terrorist considerations (From CBRN to cyberterror);
- At least one variable (the information revolution) is likely to facilitate the pursuit of cyberterrorism.

The following section analyzes in detail the specific variables affecting the future utility of cyberterror. These variables are principally related to the spread of the information age. Specifically, global connectivity, increasing information technology (IT) use, the low cost of entry, and the lack of legal consensus all present opportunities for potential cyberterrorists. Conversely, the continued utility of traditional terrorist methods, increasing cyberterror

---

[39] See Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), pp. 185-205.

[40] See Richard A. Falkenrath, Robert D. Newman, and Bradley Thayer, *America's Achille's Heel: Nuclear, Biological, and Chemical Terrorism and Covert Attack* (Cambridge: MIT Press, 1998); Jessica Stern, *The Ultimate Terrorists* (Cambridge: Harvard University Press, 1999); and The CSIS Task Force Report, *The Nuclear Black Market* (Washington, D.C.: CSIS, 1996).

[41] Falkenrath, Newman, and Thayer, pp. 18 - 26.

defensive capabilities, and uncertainty are likely disincentives to existing organizations considering cyberterror. Interestingly, the rapid change of technology and the prospects for anonymity offer a mixed set of incentives and disincentives for pursuing cyberterror.

C. Incentives for Pursuing Cyberterror

The following factors are likely incentives for pursuing cyberterrorism.

1. Global Connectivity

Offers an expanding set of options compared to previous avenues

- Diverse systems; not limited to the Internet.
- Degree of infrastructure development and connectivity vary greatly.
- Provides potential stand-off attack capability.
- Increases the number of potential targets.
- Reduces cost and complexity of command and control and propaganda dissemination.
- Provides a larger audience for terrorist acts.
- Provides an avenue for the broad dissemination of propaganda.

Global connectivity enhances the utility of cyberterror by increasing the number of possible targets and improving the efficiency and/or effectiveness of cyberterror support activities. A review of the *International Telecommunications Union (ITU) Yearbook of Statistics* shows that telecommunications networks are expanding.[42] The demographics of this expansion, particularly regarding the pace and manner in which global connectivity is being achieved, yields interesting insights. First, the growth rate in connectivity varies significantly around the globe. Second, the world is "connecting," but in a heterogeneous fashion. These insights affect the incentives for pursuing cyberterror attacks and support activities in interesting ways.

[42] International Telecommunication Union, *Yearbook of Statistics, Telecommunication Services, 1988-1997* (Geneva Switzerland: ITU, 1999).

One measure of connectivity, the Internet (a subset of telecommunication networks) offers a revealing example of the disparity between different regions. In 1998, Americans represented 52 percent of worldwide Internet users.[43] No other country comes close to reaching that percentage. This usage helps drive the U.S. demand for the sale and manufacturing of IT products, a market the U.S. also dominates - representing almost 40% of the worldwide market between 1985-1995.[44] A look at geographical regions shows the lack of use outside of developed countries. North America covers 56 percent of the world usage with Europe and Asia coming in a distant second (22%) and third (17%) respectively.[45] The regions of the Middle East and Africa, as aggregate entities, do not even make the top 15-country list. On a world scale, the Middle East accounts for 0.51 of one-percent of Internet users, and Africa accounts for only 0.74 of one-percent.[46]

Looking at Internet distribution from the hardware perspective is just as revealing as looking at user distributions.

> Internet disparity is much greater than for telephone lines. While the gap in the level of teledensity (telephone lines per 100 inhabitants) between developed and developing nations has diminished over time, new gaps have opened up for Internet connectivity. For example there are more hosts in Finland than all of Latin America and the Caribbean, there are more hosts in three developed countries of the Asia-Pacific region (Australia, Japan, and New Zealand) than in all the other countries combined and there are more hosts in New York than in all of Africa. [47]

Even with the above-described discontinuity in telecommunication network development, the technical ability to communicate via fax, telephone, or modem from anywhere on the planet still exists. What changes with location is the price of connectivity: low in advanced societies, but expensive in less developed markets. At locations where actual land-based telecommunication networks cease to exist, the opportunity to use satellite communications remains (although at much greater relative cost and higher risk of exposure).

---

[43] Computer Industry Almanac as quoted in the CyberAtlas web site. http://cyberatlas.internet.com/big_picture/geographics/article/0,1323,5911_150591,00.html

[44] Organization for Economic Co-operation and Development, *Information Technology Outlook 1997* pp. 15-19 retrieved from http://www.oecd.org/dsti/.

[45] Organization for Economic Co-operation and Development, *Working Party on Telecommunication and Information Services Policies,* Internet Infrastructure Indicators, 28 Oct 1988, retrieved from http://www.oecd.org/dsti/.

[46] Computer Industry Almanac 1998 report as quoted in NUA Internet Surveys web site, http://www.nua.ie/surveys/.

[47] International Telecommunication Union, *Challenges to the Network Internet for Development* (Geneva: ITU, 1999), p. 23.

Global connectivity enhances the attractiveness of cyberterror attacks by increasing the number of possible targets. Increasing connectivity also translates into a potentially larger audience for these attacks.

Global connectivity also enhances the attractiveness of IT for terrorist support activities. A number of violent groups have already chosen to take advantage of this opportunity. During the seizure of the Japanese Embassy in Lima, Peru, the Tupac Amaru Revolutionary Movement (MRTA), employed IT support when they developed and used a multi-media website to keep their supporters informed while broadcasting their views to an international audience. Many other violent groups use the Internet in a support role. [48] In fact, a separate survey identified 489 violent groups on the Internet, ranging from groups within advanced societies such as the U.S. to groups geographically located in remote regions of the world such as the Free Papua Movement (OPM) in Irian Jaya.[49] With IT support, terrorist organizations can communicate globally and instantaneously to enhance their command and control while using commercially available encryption methods (e.g. Pretty Good Privacy – PGP) and services. The Animal Liberation Front reportedly uses PGP encrypted email to coordinate and share information between its North American and European cells.[50]

However, the opportunities made available by the growth in connectivity do not come without some cost. The discontinuity within this growth will limit both what can be targeted, where it can be targeted and how. Because of discontinuous and heterogeneous telecommunications expansion in such places as Africa, Asia and the Middle East, the pursuit of a cyber-capability is likely to be constrained. As the demographic data presented indicate, there is a finite set of potential "jumping-off" points available to terrorists operating in less developed areas of the world. Likewise, the network access which would support Internet traffic from these regions is also limited. In the absence of having Internet access, some areas must rely on more expensive, and easily traced, traditional telecommunications systems. In effect, though the growth in connectivity suggests the absolute dissolution of traditional boundaries and distances, it is still limited to a definable set of geographic possibilities.

---

[48] Taliban Islamic Movement at www.ummah.net/taliban, the Zapatistas at www.ezln.org or the Colombian ultra-right death squads at www.colombialialibre.org . Some organizations maintain digital connections closer to home. Listed from Berkeley, CA is the Committee to Support the Revolution in Peru (Shining Path support) www.csrp.org from which you can order a "digitally remastered (compact disc)...of traditional folk music from Peru set to lyrics of the revolutionary struggle – along with voices of revolutionary fighters and prisoners."

[49] A. P. Iuris, "Information Terrorism," *Jane's for Intelink - Terrorism: A Global Survey*, 01 May 1997.

[50] A. P. Iuris, "Information Terrorism," *Jane's for Intelink - Terrorism: A Global Survey*, 01 May 1997.

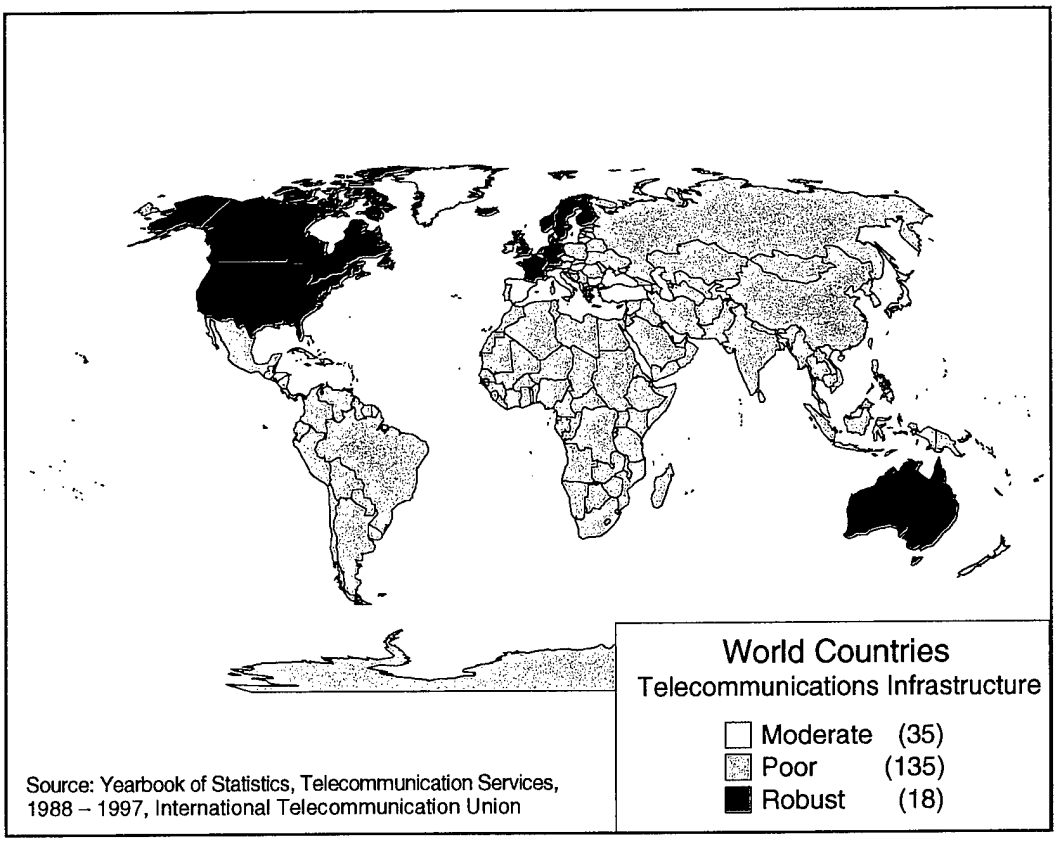


Figure 3-3: Teledensity of World States

2. Increasing Dependence on Information Technology

Highlights a potential asymmetry that was not otherwise available

- IT is widespread in the United States and other developed nations.
- Introduces new vulnerabilities.
- Increases the consequences of cyberterrorist acts.
- Provides a potential means for financial support.
- May increase the vulnerability of terrorist organizations who employ it.

> [T]echnology and change produce better service at lower cost, new markets and more efficient processes throughout the nation and indeed the world. As a result, we depend more than ever on infrastructure services. [51]

The increasing employment of IT enhances the attractiveness of cyberterror by creating more lucrative target sets and expanding the scope of potential damage. The President's Commission on Critical Infrastructure Protection (PCCIP) warned of the vulnerabilities to our national infrastructure and the dangers of increasing dependency.[52] For the U.S., all critical infrastructures are increasingly reliant on information technology. Telecommunications networks, themselves controlled by information technology, provide vital links for other infrastructures such as banking and finance, energy, transportation, and vital human services. The impact of IT on the financial industry has been significant:

> Walter Wriston, a former head of Citibank, points to what he terms a new 'information standard' that is replacing the gold standard. He contends that information about money is becoming more valuable than money, as electronic data shifts around the world instantly without any bullion or currency physically changing hands. [53]

The economic stability of the United States is a vital element of national security and global stability; the disruption of these infrastructures could have serious economic and security implications. The spread of IT to banking, finance, and commerce also presents terrorist with the opportunity to use fraud and theft for financial support of their operations.

The increasing dependency on IT may also affect terrorist organizations that choose to employ these technologies. They may increase their own vulnerability to infrastructure disruption and other information warfare techniques. As terrorist organizations become more reliant on IT, they may even become less willing to disrupt infrastructure, lest it disrupt their own operations – unless they can carefully control the effects of their attacks.

The increasing dependency on critical infrastructures presents obvious opportunities for those who would target the United States and its interests.

---

[51] PCCIP, *Critical Foundations,* p. 10.

[52] Although the use of IT is an essential element of dependency, use alone does not directly translate into IT dependency. The extent of dependency is a factor of vulnerability, redundancy, contingency plans, and mitigation/recovery measures.

[53] A. P. Iuris, "Information Terrorism," *Jane's for Intelink - Terrorism: A Global Survey,* 01 May 1997.

While the U.S. may have an IT dependency, other nations which exhibit much lower usage rates (as outlined above) may have a much lower level of dependency. Recognizing this point, the incentive to pursue cyberterror attacks may vary, based upon the primary target's IT dependency level.

3. Lack of Legal Consensus

Lack of consensus regarding traditional terrorism and computer crime offer potential offenders a safe-haven

- There are nine major multilateral conventions related to states' responsibilities for combating terrorism. The United States is a party to all of these. However, none of them explicitly covers acts against information systems. [54]

- Despite agreements to cooperate against terrorism, there is no international legal consensus or agreement on computer crimes.

- The United States has extradition treaties with 107 countries.

- It is difficult to establish conclusively the identity of the perpetrators of computer crimes.

There is a real, yet largely unrealized, opportunity for terrorists to exploit the lack of legal consensus regarding computer crime and terrorism. There is a growing international legal consensus and diplomatic efforts against conventional acts of terrorism, but response, renditions, and extradition can still be difficult.[55] The complete lack of consensus with regard to computer crimes, combined with global connectivity, means that cyberterrorists may be able to operate without the threat of arrest and extradition. There are numerous incidents of countries refusing to extradite hackers caught red

---

[54] See the list maintained by the U.S. Information Agency at http://www.usia.gov/topical/pol/terror/conven.htm

[55] The case of Abdullah Ocalan, the Kurdish separatist leader is instructive. Despite the fact that he was wanted in Turkey, he was able to travel rather freely in Europe. In fact, the Italians may even have been complicit in his escape to Kenya, where he was eventually caught. Even this capture of a well known terrorist leader caused an outcry and resulted in rioting by Kurdish emigrants in some European cities. The U.S. Government continues to emphasize bringing "terrorists to justice for their crimes and successfully conducted three renditions and one extradition in 1998, twice as many as 1995 and 1996 combined. See Dept. of State, *Patterns of Global Terrorism: 1998,* Introduction, p. 1.and Table: Extraditions and Renditions of Terrorists to the U.S. 1993-1998.

handed.[56] Using cyberterror, terrorists can attack from anywhere on the globe with relative immunity because cyberspace transcends national boundaries. Furthermore, victims of attacks may be powerless to respond to attacks launched from these safe havens, even if the perpetrators were positively identified.[57]

In the current international environment, there exists no consensus as to what constitutes computer crime as it relates to terrorism. Furthermore, within a number of states, the issue of computer crime remains unclear. Drawing on how long it has taken the international community to learn to cooperate in opposing traditional terrorism, it is safe to forecast that cyberspace-based malfeasance will persist for some time.

4. Low Cost of Entry

Relatively small investment provides a force multiplier and a limited capability

- The cost of computer hardware continues to decrease.
- Advanced hacking tools which require only minimal knowledge are freely available on the Internet.
- You get what you pay for – a low-budget capability is likely to produce low-budget results.

The cost-effective nature of cyberterror support and the low start-up costs for simple-unstructured cyberterror allow financially constrained terrorist organizations an effective, low-cost force multiplier. Cyberterror support requires little investment and returns can accumulate immediately. With a small investment (just a few thousand dollars), a group can purchase the hardware tools necessary to begin employing cyberterror. Already, Jane's Information Group is reporting that terrorists are using cyberterror support to

[56] The case of Ehud Tenenbaum ("The Analyzer"), apprehended in Israel and wanted by the United States in connection with the Solar Sunrise incident, is among the most prominent. Despite recent turbulence in U.S.-Israeli relations, Israel is a staunch U.S. ally and they still refused to extradite Tenenbaum. See also Dorothy E. Denning, *Information Warfare and Security* (Reading: Addison–Wesley, 1998), pp. 47 & 51.

[57] Listed in Appendix B are the nations with which the U.S. Government maintains bi-lateral extradition treaties. Source: www.usdoj.gov/usncb/extradite.htm. Appendix C lists the 185 member states of the United Nations. As of July 1999, the U.S. Government does not maintain bi-lateral extradition treaties with 79 UN member states. Notably included within the 79 are Afghanistan, Iran, Libya, North Korea, Sudan, and Syria.

"co-ordinate operations and to disseminate propaganda."[58] Access to other support requirements such as weather, maps, and travel related information is also available on demand. Chat rooms link hackers of different skill levels creating a virtual classroom for learning and exchange of success stories.

The Internet is a rich source of malicious software; a variety of tools are freely available for downloading. However, unless the source code is available and someone in the organization has the requisite knowledge to verify what it will do, it is risky to use this type of software. It may well perform as advertised but it is also possible that the tool may be a Trojan horse[59] that could damage the user's system.

The rapid pace of change noted above also contributes a lower cost of entry in some cases by preventing effective security measures. Some system administrators may be overwhelmed or complacent and fail to change the default settings of new systems and software. This allows attackers to gain access using the default login and password combination. This lowers the cost of entry by reducing the knowledge and resources necessary to target some systems.

For terrorists, a simple-unstructured cyberterror attack may require minimal investment, but the results will also be constrained in their effects. The vulnerable systems may not have any tactical or strategic significance. As the level of cyberterror attack increases the costs of intelligence, human capital, and in some cases processing power, escalate as well. The United States, with its enormous human and technological resources has attempted to create an offensive IW capability. Yet, after several years and millions of dollars, this capability may not yet have reached an operational status.[60]

In review, the low cost of entry holds true if the capability sought is intended to accomplish simple-unstructured cyberterror support or attacks. However, the cost of entry will increase for both advanced-structured and complex-coordinated cyberterror attacks.

D. Disincentives to Pursuing Cyberterrorism

While the previous section examined the factors that may induce terrorist organizations to diversify into cyberterror, this section examines some of the

---

[58] A. P. Iuris, "Information Terrorism," *Jane's for Intelink - Terrorism: A Global Survey*, 01 May 1997.

[59] A Trojan horse is malicious software contained within an otherwise useful program.

[60] William M. Arkin, "A Mouse that Roars?" Special to *washingtonpost.com*, 7 June 1999, http://www.washingtonpost.com/wp-srv/national/dotmil/arkin.htm

factors that may reduce their incentives. The availability and effectiveness of strategic alternatives, an increasing emphasis on the protection of infrastructures, and overall uncertainty regarding the effectiveness of cyberterror all provide disincentives.

1. Strategic Alternatives

Cyberterrorism is one of several strategic options available to contemporary terrorist organizations

- Terrorists have multiple strategic options but limited resources.
- A large supply of soft targets means that their traditional methods are still viable.
- Cyberterror does not have the potential to produce mass casualties.
- Achieving a level of cyberterror capable of producing similar spectacular results requires a significant investment.

The utility of cyberterrorism may be lessened by the presence of strategic alternatives for existing terrorist groups. The strategic alternatives include traditional terrorist operations (bombings, hijackings, kidnapping, assassination, etc.) and chemical, biological, radiological, and nuclear weapons (CBRN).[61]

Cyberterror has the potential to cause widespread disruption; but its actual physical effects are limited. It does not currently have the capability to cause widespread destruction. The principal consequences of a cyberterror attack include a loss of reputation and confidence (psychological), a loss of proprietary information and privacy, and a loss of money or capital (financial). In most cases, the risk to information systems is not directly related to the risk to human life. There are some exceptions, and it is possible that widespread disruption can increase mortality indirectly. However, the physical harm that can be inflicted by cyberterrorism does not approach that possible using CBRN.

Of course, some terrorist groups may pursue limited cyberterror capabilities in order to enhance their ability to conduct conventional operations. Similarly,

[61] See Falkenrath, Newman, and Thayer pp. 14-18, for a description of these weapons. Note that the use of this acronym does not mean that this is an all-in-one package. Each component has specific resource requirements and implications.

they may pursue limited cyberterror capabilities to facilitate access to the resources necessary to develop CBRN weapons. While a terrorist organization could conceivably pursue each of these alternatives, it is unlikely because of resource constraints. Terrorist organizations have limited resources and are generally averse to increased risk, since their risk level is high enough already. Pursuit of complex-coordinated cyberterror capabilities may reduce rather than enhance their capability to conduct other operations, because of the potentially high resource requirements. It is also unlikely that groups that have dedicated themselves to the pursuit of more lethal and destructive weaponry would view mass disruption as essential to their efforts. If it is not perceived as essential, few terrorist organizations have the resources to afford luxuries.

The continuing utility of traditional terrorist methods represents a disincentive to the potential use of cyberterror. The increasing attention or focus on CBRN terrorism and cyberterrorism may actually result in increased opportunities for terrorist organizations that utilize more traditional means and methods. They may be able to operate "below the radar" of law enforcement agencies that are increasingly concerned with more exotic forms of terrorism. Terrorist organizations "seem to prefer assurance of modest success to more complicated and complex- but potentially higher pay-off (in terms of casualties and publicity) operations."[62] The lure of traditional methods may be sustained by the increasing lethality of conventional weaponry. This would potentially enable greater efficiency for terrorist organizations.

2. Counterterrorism Forces

Two factors make it likely that anti-terrorism and counter-terrorism will improve significantly

- The increased awareness of vulnerabilities (as a result of Y2K, PCCIP, etc.) will likely lead to improved defenses.

- The capabilities and resources of counterterrorist forces are increasing.

One threat to the potential of cyberterror is the growth of defensive capabilities. In the absence of a superpower threat, there has been an increasing focus on terrorist threats. There is a growing awareness in both the private and public sector of vulnerabilities and dependencies associated with information systems. The President's Commission on the Critical

[62] Bruce Hoffman, *Responding to Terrorism Across the Technological Spectrum,* presented to the Fifth Annual Conference on Strategy at the US Army War College Carlisle Barracks, PA, 15 July 1994.

Infrastructure Protection (PCCIP) report and the potential for Year 2000 (Y2K) computer problems has increased awareness of information system vulnerabilities and dependencies and may decrease the cyberterrorist's window of opportunity. Computer Emergency Response Teams (CERTs) and similar organizations have improved their structure and procedures to identify system violations and respond with the appropriate countermeasures. The response time to system attacks is improving with each attack by typical hackers. A prime example is the rapid reaction to the "Melissa" macro virus.

Terrorist organizations that use information technology for improved command and control are as vulnerable as any other organization to monitoring and intrusion. The use of strong encryption will provide some protection but, like other organizations, they are vulnerable when the improperly trained user does not follow proper procedures. Their use of information technology may help counterattackers locate and track terrorist operatives. Internet use can leave an electronic map back to the user and mobile telecommunications systems can provide a beacon for counterattack forces. Counterterrorist forces could potentially use information warfare tactics against the terrorist group to negate or manipulate their action without the group realizing it.

3. Uncertainty

The utility of Cyberterror is still unknown

- It is unclear whether disruption is a suitable substitute for destruction.
- Cyberterror may be an adjunct to destruction but the reliability and "half-life" of any attack tool can be limited; a capability may become obsolete in a short period of time.
- The results of a cyberterror attack are difficult to predict.
- With limited resources, terrorist organizations may be unwilling to pursue a capability with so much uncertainty.

The greatest uncertainty that accompanies the use of cyberterrorism is operational - will the attack or collection program achieve the desired results? This uncertainty represents another disincentive to cyberterror. While it may introduce new vulnerabilities and dependencies, it can also introduce new security measures and eliminate existing vulnerabilities. The information technology industry continually produces new security measures to eliminate existing vulnerabilities; hardware and software upgrades or merely better

security procedures, can quickly plug many security holes. An effective attack tool or methodology may rapidly lose its effectiveness as awareness increases and countermeasures are developed and implemented. Terrorist organizations that are constrained by resources might expend a great deal of resources acquiring a capability that may be only marginally useful by the time it is fully operational because of the rapid pace of change.

The pace of change means that tools for cyberterror attack and support may not achieve the desired effects. In some cases, the effects may be easily predictable. However, in many cases the primary and secondary effects of disrupting an information system may not be so easily predictable. The potential for "blowback" because of unintended consequences cannot be ruled out – therefore contributing to uncertainty. A logic bomb may not receive the required sequence of events to carry out its programmed intent. Additionally, efforts to cover the tracks from an attack may backfire and lead the attacked to the attacker. The terrorist group may then find itself on the defensive instead of the offensive.

The final and larger question regarding uncertainty is whether cyberterrorism will have the same impact as conventional terrorism. Despite some of the advantages offered by cyberterrorism, the ability to generate sufficient pressure on the adversary through disruption is still the most critical question. Given the demonstrated difficulty of coercing an adversary with physical destruction, disruption may not be considered a suitable substitute for destruction. Disruption is unlikely to be considered as a unilateral objective when the adversary has resorted to force against non-combatants to counter terrorist operations (as was the case in Kosovo).

Despite all of the attention surrounding cyberterror, nobody has successfully demonstrated the capability to use these types of attacks to coerce and create fear comparable to conventional terrorism. First, even conventional terrorist tactics have a poor track record of achieving their ultimate goals. Second, critical infrastructure components are subject to disruption on a regular basis as a result of natural phenomena, accidents, and operator error. Nevertheless, most individuals and organizations devise ways to deal effectively with these disruptions. It is natural to ask what scale of disruption would be necessary to achieve the goals of terrorist organizations. This is not to say that it is impossible with cyberterror, only that it has not happened yet and therefore it is unproven. This lack of proven efficacy contributes to uncertainty for terrorist groups thinking about moving into the cyber-realm.

E. Factors Acting as Both an Incentive and Disincentive

Whereas the previous sections addressed factors that were clearly positive, or negative, incentives for pursuing cyberterror, the following factors are less

clearly defined. Both rapidly changing technologies and anonymity offer a combination of incentives and disincentives for pursuing cyberterrorism.

1. Rapidly Changing Technology

Terrorist organizations may potentially profit or be victimized by the vulnerabilities associated with rapidly changing technologies

- Technology is changing at unprecedented rates.
- Profit and efficiency, not security, are the primary considerations.
- New technologies can introduce vulnerabilities that are not always well understood.
- The pace of change prevents users and administrators from understanding and implementing proper security measures.
- Standardization of technology for effectiveness and economies of scale tends to standardize the vulnerabilities available to an adversary.

New software and hardware introduce the possibility of new security vulnerabilities. The rapid pace of change means that the vulnerabilities of new technologies are not always well understood and that many users and administrators may be poorly trained in proper security measures. This potentially translates into more security vulnerabilities for cyberterrorists to exploit. It also imposes a requirement for terrorist organizations to keep current with technology changes if they wish to exploit them.

The demand for new information technologies is commercially driven; government has taken a backseat to private industry. Corporations often maintain their competitive edge by continually integrating new technology into their operations. Most organizations, including the Department of Defense and government agencies, employ commercial-off-the-shelf (COTS) technologies. However, this rapidly changing technology can create vulnerabilities without

owner or operator's knowledge or consent.[63] Even program fixes or patches may open the doors to exploitation in other program areas. Further, the standardization of technology for effectiveness and economies of scale tends to standardize the vulnerabilities available to an adversary.

The pace of change places a burden upon both users and system administrators charged with maintaining security. In addition to managing day-to-day operations, they must keep abreast of newly discovered vulnerabilities, threats, and countermeasures. While there has been an increase in awareness and use of security measures,[64] any system connected to a network with remote access can never be completely secure.

If terrorist organizations wish to pursue cyberterror attacks above the simple-unstructured level then they must learn to incorporate and understand the rapidly occurring changes in Information Technology. Like other organizations that use IT, terrorist organizations must be aware of their vulnerabilities and ensure that their own use of IT does not become a security liability.

2. Anonymity

Anonymity may be achieved, however not without risk

- Long distance communications allow parties to remain relatively anonymous.

- From the target perspective, it is difficult to immediately distinguish a cyberterrorist attack from other malicious activity.

---

[63] Systems change so fast that programmers must build compatibility features into software to ensure proper functioning with previous and future standard systems. Microsoft for example, in an effort to allow Windows NT Server 4.0 to link to any other operating system, contains a flaw in its security function. The flaw gives anyone with standard access to the server services the ability, under certain conditions, to alter any file. All this provides the potential for unauthorized access or use for group exploitation. As more systems compete on the open market, assimilation of the operating systems is key to keeping the seamless operation of the information highway. This means that all systems must operate under the same guidelines, and these guidelines will bring more problems like those faced by Microsoft for the cyberterrorists to exploit.

[64] Current statistics reveal that nations with the higher Internet usage rates also have a higher rate (per 100 000 inhabitants) of secure web servers for electronic commerce. "The United States is a clear leader with three quarters of all electronic commerce sites and also has the highest number of secure web servers at 6.1 per 100 000 inhabitants." OECD, *Working Party*, p 10.

- The difficulty in positively identifying the location, identity and intent of an attacker can delay or prevent an effective response, giving an edge to the attacker.

- Anonymity is not absolute; calls and connections can be traced and computer intrusions detected.

- Anonymity is not always possible or desirable for terrorist organizations.

The use of cyberterrorism may allow terrorist organizations greater anonymity. Theoretically, there are two levels of anonymity – organizational and individual; cyberterrorism could potentially enhance both. For obvious reasons, individual anonymity has always been an imperative for terrorist organizations. Access to the telecommunication's networks and their growing complexity provide ample cover for terrorist groups. Individual terrorists can perform malicious acts or collect information on critical infrastructures while continually changing locations around the world. Traceroutes of Internet routing show the development of network avenues throughout the world, which terrorists could use as jumping points for dispersed field operators or a means to cover their tracks. As the Hanover Hacker case demonstrates,[65] hackers may use various network connection paths, but the threat of discovery and apprehension remains.

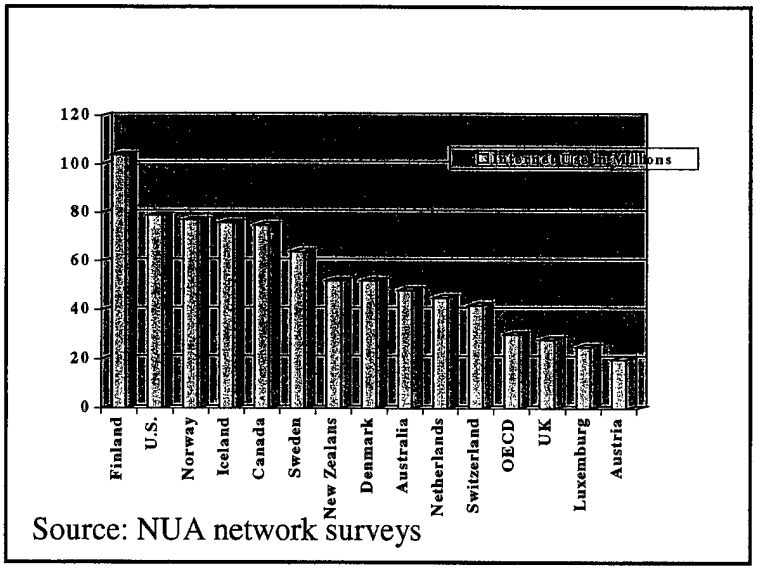


Figure 3-4: Traceroutes for Network Capacity 1998

[65] Described in detail in Clifford Stoll, *The Cuckoo's Egg* (New York: Pocket Books, 1990).

Improved organizational anonymity could potentially benefit some terrorist organizations by allowing them to take action with plausible deniability. This may be useful for attempts to manipulate other parties into military action against each other. The "Solar Sunrise" incident offers a glimpse into the possibilities.[66] One possible scenario might involve Taiwanese nationalists, conducting attacks that appear to originate in China in order to prod the United States into retaliatory action. However, terrorist groups must communicate their demands as an essential part of any coercive or deterrent strategy and this usually involves (explicitly or implicitly) identifying the organization. The exception may be religious or anarchist groups that really have no demands, only objectives that are not dependent upon the actions of the victims.

The potential for anonymity during support operations could also be highly beneficial. It may allow terrorist organizations to gather information with much less risk than conventional reconnaissance. Additionally, unlike cyberterror attack, where the terrorist's network activity is illegal, terrorist IT support activities can be legal, cost-effective, and time efficient.

F. Summary

What is the supply side of cyberterrorism?

This section highlighted the factors facilitating the use of traditional terrorism as well as other forms such as CBRN and cyberterror. This was the first phase of analyzing the supply side of cyberterrorism.

Global factors outlined earlier in this chapter emphasize the continuing utility of terrorism. The changing world security environment has resulted in greater uncertainty in which ethnic tensions and quests for autonomy are rising. The growth of non-state actors such as TCOs, MNCs and NGOs are free to create alliances or independently operate unconstrained by state influence or boundaries. The proliferation of CBRN weapons offers terrorist organizations access to greater destructive power than ever before. Lastly, the information revolution is creating an environment in which a terrorist may leverage informational vulnerabilities previously not possible.

---

[66] This February 1988 incident involved attempts to penetrate DoD computer systems during a period of increased tensions with Iraq. Because DoD officials were initially unable to identify the source of the attacks, they believed that the Iraqis could have been responsible and considered military options to respond to the attacks. The perpetrators were eventually identified as an 18 year old Israeli hacker, Ehud Tenenbaum, and two teenage protégés in California.

Terrorists will likely seek to capitalize on the specific opportunities presented by the information revolution. Global connectivity, information technology dependence, international legal loopholes and low entry costs collectively may contribute to newer forms of terrorism. If in demand, terrorists may benefit from these factors by pursuing capabilities aimed specifically at disrupting these vulnerabilities.

As numerous studies have predicted, the widespread disruption of information systems and critical infrastructures could indeed have grave consequences. However, developing a capability to accomplish this requires a great deal more than just a "computer, modem, telephone, and user-friendly hacker software."[67] The viability of traditional terrorist methods as well as other new forms of terror (i.e. CBRN), the uncertainty regarding the efficacy of cyberterrorism, the limited resources of terrorist organizations, and other considerations outlined in this chapter suggest that a more sobering view of the supply-side of cyberterror be taken.

[67] PCCIP, *Critical Foundations*, p. 15.

IV. The Decision to Pursue Cyberterror: Factors and Influences

A. Introduction

While the previous chapter identified the incentives for and disincentives to the pursuit of cyberterror, this chapter attempts to determine what types of terrorist organizations are most likely to take advantage of these opportunities. By definition, all terrorist organizations have demonstrated the motivation and intent to effect political or social change through violence. However, the targets, methods and scope of violence vary widely. Terrorist organizations are constrained by resources, their goals, and their specific operating environment. They must choose tactics and targets that they perceive as appropriate. Not every terrorist organization pursues chemical weapons; likewise, not every organization will pursue cyberterrorism. Each organization must determine the degree to which the disruption of information systems and critical infrastructures supports its goals. Therefore, even if a terrorist organization recognizes the opportunities and threats, it still must decide whether to take advantage of the opportunities and adopt cyberterrorism.

There are several approaches to analyzing and understanding terrorism and terrorist acts: a strategic, a psychological, and an organizational analysis.[68] Each of these approaches represents a valid and valuable analytical approach but none of them possesses complete explanatory power.[69] It is possible that cyberterrorism may not have any strategic utility for a particular group, yet it may fulfill the organizational or psychological needs of either individuals or the organization as a whole. Conversely, cyberterrorism may be congruent with their ideology, yet may be unappealing to the group or key individuals within the organization. Therefore, in order to understand the potential utility of cyberterrorism, and the likelihood that it will be adopted as a tactic, it is important to recognize the impact that its adoption may have on

[68] It is important to emphasize that the analysis conducted in this study does not apply these perspectives to the origins of terrorist organizations but rather to the decision –making processes in existing organizations.

[69] Walter Reich, *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*, ed. Walter Reich (Washington, D.C.: The Woodrow Wilson Center Press, 1990), pp. 2-3.

each of these dimensions. In this chapter, we analyze the decision to adopt cyberterrorism from the strategic and psychological perspectives.[70]

The first section analyzes the utility of cyberterror from a strategic perspective. Because terrorist groups with similar ideologies have similar strategic goals, the strategic utility of cyberterrorism is examined with respect to particular ideologies. This examination is done without regard to resource constraints, which are addressed in Chapter V. The second section examines the potential effects of individual motivations and group dynamics on the decision to pursue cyberterror. It contrasts the motivations of terrorists, computer hackers and information technology professionals and highlights the challenges and implications of trying to integrate hackers and technical professionals into a terrorist organization. The final section examines the potential impact of organizational factors, such as structure, culture, and organizational lifecycle, on the decision to pursue cyberterror.

A word of caution is necessary before addressing these issues. Terrorism is obviously a complex phenomenon; scholars cannot agree on a definition, let alone on the reasons for the adoption of terrorism as a strategy. The same difficulty applies to understanding terrorist decision-making; i.e. why and how terrorists select tactics and targets. It is important to keep in mind that there are wide variations in motivations and tactics among terrorist groups, even among those that share similar ideological goals. We realize that the characterizations of strategic goals, targeting preferences, psychological motivations, and organizational goals offered below are generalizations. Further, we understand that our analysis may not be applicable to every group under all circumstances. However, these judgments are a necessary first step in focusing further investigations of the potential utility for cyberterrorism.

B. Strategic Analysis

One method of analyzing the purpose of terrorist acts is to examine them in a strategic context; i.e. how the acts relate to the stated strategic goals of the terrorist organization.[71] These strategic goals may include destabilization, coercion, deterrence, revenge, and defense against competing groups or

---

[70] Application of organizational life cycle analysis and other specific organizational areas, although introduced in this chapter, were not applied to our framework. These areas did not lend themselves to a general application of terrorism or terrorist ideologies. Likewise, our research did not uncover sufficient data to support such a level of analysis. However, portions of organizational life cycle analysis are incorporated in Chapter Six's analysis of implementation options.

[71] Martha Crenshaw, "The Logic of Terrorism: Terrorist Behavior as a Product of Strategic Choice," *The Origins of Terrorism*, ed. Walter Reich (Washington, D.C.: Woodrow Wilson Center Press, 1990), pp. 7-24.

counterterrorist forces.[72] Tactics that garner publicity and international support (political, material, or financial), weaken domestic support for or destabilize the regime or policies that the terrorists oppose, can support these strategic goals.

This approach assumes that terrorist organizations possess a collective rationality and select courses of action from a set of perceived alternatives.[73]

> Efficacy is the primary standard by which terrorism is compared with other methods of achieving political goals. Reasonably regularized decision making processes are employed to make an intentional choice, in conscious anticipation of the consequences of various courses of action or inaction. Organizations arrive at collective judgements about the relative effectiveness of different strategies of opposition on the basis of observation and experience, as much as on the basis of abstract strategic conceptions derived from ideological assumptions.[74]

Although this passage specifically refers to the decision to adopt terrorism versus other means of effecting political change, it can be extended logically to the process of selecting weapons, tactics, and targets. However, the excessive violence and seemingly random nature of some terrorist acts leads many casual observers to question the rationality of terrorists. To a large extent, this conclusion is based on mirror imaging; i.e. assuming that terrorists reason based on the same premises as their adversaries. The continuing use of terrorism does not necessarily reflect terrorist irrationality, but rather reflects an inability to understand clearly the premises of terrorist logic.

---

[72] It has also been suggested that terrorists may have an interest in provoking disproportionate retaliation, to both gain additional publicity and demonstrate the veracity of the charges against a state. This may be particularly true in cases involving repression of an ethnic group. See Martha Crenshaw, "The Causes of Terrorism," *Comparative Politics* (July 1981): p. 387.

[73] Crenshaw, "The Logic of Terrorism," p. 8. See also J. DeNardo, *Power in Numbers: The Political Strategy of Protest and Rebellion* (Princeton: Princeton University Press, 1985).

[74] Crenshaw. "The Logic of Terrorism," p. 8.

> In reality, there is a great deal of territory between irrationality and rationality. Moreover, rational terrorists may reason quite logically, but the fixed premises that are the basis of the rational calculus can lead to a "psycho-logic" with dreadful consequences. [75]

According to Bruce Hoffman, "All terrorist groups seek targets that are rewarding from their point of view, and employ tactics that are consonant with their overriding political aims."[76] Therefore, it is necessary to examine cyberterrorism in the context of espoused goals.[77] Because time and space do not allow a group by group analysis, we have adopted the common practice of categorizing terrorist groups by their dominant ideology.[78] The following sections examine the strategic utility of cyberterror for five types of terrorist organizations: ethno-nationalist/separatists, revolutionary, far-right, new age (single-issue), and religious.[79]

1. Ethno-Nationalist/Separatist (ENS) Terrorism

ENS terrorists principally seek to achieve political autonomy, usually in the form of a separate state, or work towards the "elevation of the status of one communal group over others."[80] Nationalist groups may also work "to oppose foreign influences in their countries."[81] ENS terrorist organizations typically

---

[75] Jerrold M. Post, "Prospects for Nuclear Terrorism: Psychological Motivations and Constraints," *Preventing Nuclear Terrorism*, ed. Paul Leventhal and Yonah Alexander (New York: Lexington Books, 1987), p. 92.

[76] Hoffman, *Inside Terrorism,* p. 158.

[77] We recognize that the specific features of an espoused ideology may be vague or inconsistent. Nonetheless, it is possible to classify terrorist organizations by ideology and derive some useful insights from the common denominators of these broad ideological categories.

[78] Ideology is used in a general sense as "the body of doctrine or thought that guides an individual, social movement, institution, or group." *Random House Webster's Collegiate Dictionary* (New York: Random House, 1991), p. 668. We recognize the difficulty of categorizing the complex activity of terrorism and the fact that not all of these categories are mutually exclusive. In reality, some groups may adopt ideologies that represent a hybrid of the ideological categories that we have chosen. Our effort is not to identify a pure ideological type, but only to assign groups to the ideology that most dominates the group's activity. Additionally, we recognize that level of actual commitment to an espoused ideology may vary and that other motivations can influence terrorist operations.

[79] Adapted from Martha Crenshaw and John Pimlott, eds. *The Encyclopedia of World Terrorism, Vol. 1* (Armonk: M.E. Shapre, 1997).

[80] Daniel Byman. "The Logic of Ethnic Terrorism," *Studies in Conflict and Terrorism* 21 (Spring 1998): pp. 149-169.

[81] Noemi Gal-Or. "Nationalist Terrorism," *The Encyclopedia of World Terrorism, Vol. 1,* ed. Martha Crenshaw and John Pimlott (Armonk: M.E. Shapre, 1997), p. 192.

have great staying power and are among the longest surviving terrorist groups. The cause of independent statehood is not easily abandoned, even in the face of concentrated counter-terrorist efforts by the adversarial state and members of the international community. Examples of ENS terrorist organizations are the Provisional Irish Republican Army (PIRA), the various Sikh movements within India, the Palestine Liberation Army, the Kurdish Workers Party (PKK) in Turkey, the Basque ETA in Spain, and the Liberation Tamil Tigers of Eelam (LTTE) in Sri Lanka.

In general, the principal strategic goals of ENS groups seeking autonomy are to increase the political and financial costs of the adversarial state and its supporters and to increase the support for their cause among members of their ethnic group. These groups frequently strive to achieve publicity and possibly international recognition and support for their cause. Where ENS groups seek to limit foreign influence, they frequently attempt to increase the economic costs of businesses that are perceived to represent foreign influence.

With regard to violence, certain nationalist terrorists have shown a preference for causing numerous casualties; but overall nationalist violence tends to be more narrowly focused, especially when compared to the indiscriminate application of violence by religious extremists.[82] Symbols of authority that represent the state are typically the target of violence by nationalist terrorists. These types of targets include, but are not limited to, public officials, public facilities and utilities, members of other ethnic groups, and representatives of other governments that are perceived to oppose self-determination. When these groups seek to combat foreign influence in their country, they may target the businesses, tourists, and embassies of foreign governments.[83] However, violence against foreign nationals by ENS groups is generally limited, because these organizations require international support for their efforts. For example, none of the groups mentioned above routinely targets the United States or other nations.

ENS terrorists have also shown a desire and willingness to attack against infrastructure targets, which symbolize state control.[84] However, using cyberterror to attack infrastructure targets requires an advanced-structured or complex-coordinated capability. Being the case, it may be simpler and more

---

[82] Hoffman, *Inside Terrorism,* pp. 199-205. See also Byman, "The Logic of Ethnic Terrorism," pp. 149-169.

[83] Gal-Or, "Nationalist Terrorism," p. 193.

[84] As the *Patterns of Global Terrorism 1997-Group Profiles* highlights, following the breakdown of the 1996 cease fire the PIRA conducted a bombing campaign on the British mainland targeting train and subway stations as well as shopping areas. The Tamil Tigers, another nationalist group, have targeted public utilities in Sri Lanka – Noemi Gal-Or, "Nationalist Terrorism," p. 193.

cost effective for nationalist terrorists operating in the disputed territory to continue to use conventional attacks against these types of targets. For nationalist terrorists operating from an area external to the disputed territory (because of effective security measures or forced exile), cyberterror attacks against critical infrastructure may be a viable option. The same logic applies to attacks against the critical infrastructure of international supporters of the incumbent regime. When the selected targets are not in the immediate area of operations, cyberterror attacks offer reduced vulnerability and potentially more efficient use of resources. The table below summarizes the considerations based on the terrorist location versus the target location. [85]

		Location of Target	
		Domestic	International
Terrorist operating base	Domestic	Conventional attacks are simpler; more likely	Cyberterror attacks provide more efficient use of resources
	Inter-national	Cyberterror attacks provide access that may otherwise be unavailable	Utility of cyberterror dependent upon degree of IT use in target country. (These types of attacks are generally eschewed by nationalist terrorists)

Table 4-1: Effect of Geography on Cyberterror Utility

The issue of collateral damage (to actual or potential supporters) is significant for nationalist terrorists seeking to maintain a base of support among their constituency or the international community.

> Their 'target audience', however is not just the local, indigenous population but often the international community as well. These groups, accordingly, recognize the need to tightly control and focus their operations in such a manner as to ensure the continued support of their local 'constituencies' and the sympathy of the international community. What this essentially means is that their violence must always be perceived as both purposeful and deliberate, sustained and omnipresent. [86]

Cyberterror and its disruptive effects could potentially enhance nationalist terrorists' efforts to create and maintain a constituency and generate

[85] This classification is derived from the work of Ariel Merari, "The Classification of Terrorist Groups," *Terrorism: An International Journal* 1.3/4 (1978): pp. 331-346.

[86] Hoffman, *Inside Terrorism,* p. 161.

international support. Whereas mass violence may drive the undecided citizen from the nationalist cause, disruption may become an attractive option to gain publicity and support without alienating potential supporters, both domestic and international. Limiting damage is a relatively straightforward consideration when kidnapping and assassination are employed. However, bombings and infrastructure attacks may require more careful planning and execution to avoid collateral damage. The same considerations will likely apply when conducting cyber attacks against infrastructure targets.

> The more successful ethno-nationalist /separatist terrorist organizations will be able to determine an effective level of violence that is at once 'tolerable' for the local populace, tacitly acceptable to international opinion and sufficiently moderated not to provoke a massive governmental crackdown and reaction. [87]

Cyberterror could easily meet the standard of "purposeful and deliberate" and still be tolerable for the local population. However, lower level capabilities may not present a "sustained and omnipresent" threat. First, the capabilities at the simple-unstructured level may become obsolete as security measures are improved. Second, attacks at the simple-unstructured level may not rise above the "noise level" created by ordinary hackers or naturally occurring disruptions. A good example of this is the denial of service attacks carried out in May 1998 by the Internet Black Tigers, purportedly an offshoot of the LTTE, against e-mail servers of the Sri Lankan government. These simple attacks caused a minor disruption but were quickly countered. Since then the Internet Black Tigers have disappeared.

The low cost of entry may be an advantage for ENS terrorist organizations with limited resources or no sponsorship. However, low entry cost primarily equates to a simple-unstructured cyberterror capability. These types of attacks, may initially offer good return on a minimum investment but the long term value is questionable. The initial attacks are likely to get a great deal of publicity but will also result in improved security measures. At the simple-unstructured level, where the attacker is dependent on others to provide his tools, the ENS terrorist may not be able to circumvent this improved security. A more robust capability will require a more significant investment.

At the advanced-structured level, cyberterrorists may be able to cause greater damage and disruption but they may be unable to predict and control the effects of their attacks. Widespread disruption may succeed in providing publicity but unless the effects are controlled, it may also alienate potential supporters by exceeding their tolerance level. In areas where the terrorists are not particularly concerned with collateral damage, an advanced-structured

[87] Hoffman, *Inside Terrorism,* p. 162

capability may be useful in a supporting role for conventional terrorist attacks. At this level, cyberterror attacks could provide a tactical advantage for terrorists by degrading the command and control of counterterrorist forces. Cyberterror attacks could also be used to delay the response of emergency services. Cyberterror beyond the advanced-structured level is inconsistent with the scope of past traditional ENS terrorist acts and therefore unlikely.

The connectivity and information technology dependency of both the disputed regime and the terrorist constituency are likely to be important factors in the decision to use cyberterror. If the ENS terrorist operates within a society with minimal information-systems dependency and connectivity, then the attractiveness of cyberterror lessens due to the smaller possible realized gain. However, if the target audience is a developed society, such as Western Europe (see statistics available in chapter III), network connectivity provides access to the audience, whom the nationalist and the government are competing to influence. The growing global connectivity may provide the ENS terrorist with access to the international community regardless of where he resides. The ENS terrorist operating in another country can remain virtually "local." He can conduct cyberterror attacks from virtually any location with appropriate telecommunications access.

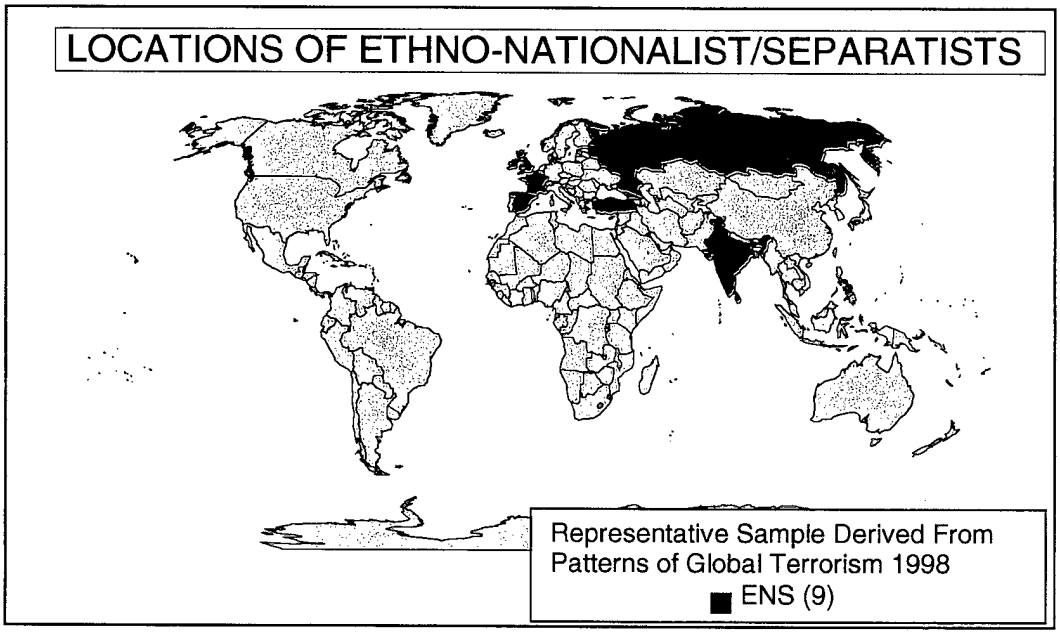


Figure 4-1

To summarize, for ENS terrorists:

- Attractiveness of cyberterror is primarily related to the information-systems dependency of the adversary.
- Continued IT use to facilitate propaganda and publicity of nationalist aims to leverage support from the international community.
- Simple-unstructured attacks are likely to prove non-coercive.
- Advanced-structured attacks can support conventional operations to provide a tactical advantage, and also be used to gain international attention.
- Mass disruption of information infrastructure and other complex-coordinated activities are unlikely.

2. Revolutionary Terrorism

Revolutionary terrorists, such as the Red Army Faction, seek to overthrow established governments as part of a broad program of social transformation. Although the political ideologies of the revolutionary terrorists can range, they are generally leftists.[88] In contrast to nationalist terrorists, revolutionary terrorists do not "seek to preserve the status quo, the aim is to change the rules of the game."[89] They are interested in a wholesale political transformation, not just the redistribution of territory for a particular ethnic group.[90]

Groups such as the German Red Army Faction (a group dominated by left-wing revolutionaries) have "selectively kidnapped and assassinated persons whom they blamed for economic exploitation or political repression in order to

---

[88] Gal-Or, "Revolutionary Terrorism," p. 194.

[89] Gal-Or, "Revolutionary Terrorism," p. 195.

[90] There is, of course, some overlap between nationalist and revolutionary terrorism. Many nationalist groups espouse a political ideology that they intend to apply to their newly created state. However, their primary goal is the establishment of that new state rather than the transformation of the existing state. For true Marxist revolutionaries, the establishment of a state on the basis of ethnic affiliation is antithetical. Nonetheless, many nationalist groups adopt a leftist ideology derived from Marxism.

attract publicity and promote a Marxist-Leninist revolution."[91] In general, "Marxist revolutionaries do not believe in indiscriminate violence."[92]

Some social-revolutionary terrorist organizations, in particular the Italian Red Brigades, have a history of targeting computer-related facilities. The Italian Red Brigades in their "Strategic Directions Resolution" of February 1978 identified computer systems as the tool of American multinationals and a link to imperialism. From the Strategic Directions Resolution:

> You see, computers are identified as a symbol, the highest profile target. It is important to destroy their mesh, to disrupt these systems, beginning from the technical-military personnel who direct them, instruct them, and make them functional against the proletariat. [93]

A statistical review, conducted in a separate study by Rozen and Musacchio, identified a total of 57 attacks against computer-related facilities between 1978 and 1988. Ninety-two percent of the attacks took place within Europe (Italy 52%, France 21%, West Germany 12%, Belgium 7%) with about half of the computer-related facility attacks within Italy attributed to the Red Brigades.[94]

Since the collapse of the Soviet Union, left-wing revolutionary movements have steadily declined.[95] With regard to the remaining left-wing movements, identifying the movement's context within its state, that is the state's relative information infrastructure development level and movement's locale within the state i.e. rural versus urban, helps discern the attractiveness of cyberterror. For example, a revolutionary movement focused in the hills of Peru, a rural location with little or no information-systems dependent infrastructure will have little use for cyberterror. As a movement begins to tackle recruitment and operations in an urban environment, the attractiveness of cyberterror increases if, and only if, the urban environment has a greater information systems infrastructure.

---

[91] Hoffman, *Inside Terrorism,* p. 157.

[92] Gal-Or, "Revolutionary Terrorism," p. 194.

[93] Quoted in Jerrold M. Post, Kevin Ruby, and Eric Shaw, *From Car Bombs to Logic Bombs: The Growing Threat from Information Systems Terrorism.* (Washington D.C.: George Washington University, 1998), p. 6.

[94] Post, Ruby and Shaw, p. 6.

[95] While the USSR did not actively support every left-wing terrorist organization, the decline and collapse of European communism did coincide with a general decrease in the level of activity by left-wing terrorist organizations in Europe. The effectiveness of counter-terrorist forces also played a significant role.

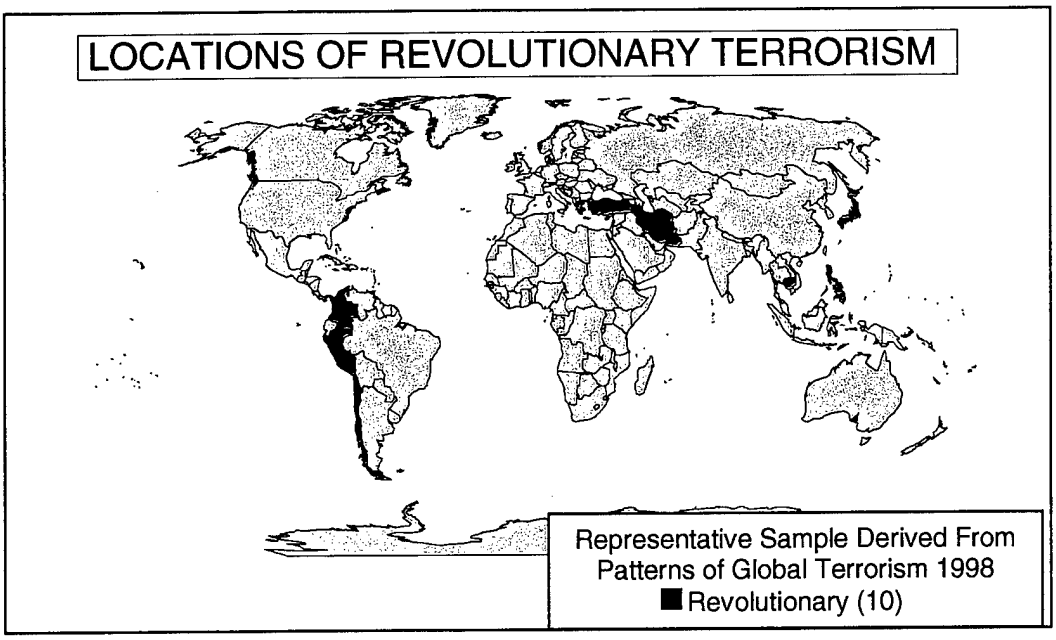


Figure 4-2

Revolutionary terrorist target selection is dominated by the symbolism of the target. Past attacks, as the one described above by the Italian Red Brigades, focused on individuals or symbols of state control. In the case presented, computer-related facilities represented the symbols of state control. However, the computer is no longer the sole province of governments and large corporations. When the Red Brigades issued their communiqué, personal computers did not exist and the Internet was still the ARPANET.[96] All this has changed though with the introduction and proliferation of the personnel computer and the Internet; this has allowed ordinary citizens access to computing power that was once only available to governments and corporations.

[96] Today's Internet is the result of US Government research on packet-switched networks. The ARPANET, developed by the Defense Advanced Research Projects Agency (DARPA) was a restricted wide area network that connected military, university and research computers. In the 1970s, DARPA adopted the TCP/IP protocol suite that is at the heart of the current Internet. For a brief history of the Internet, see Barry M. Leiner, et. al, *A Brief History of the Internet*, available online at http://www.isoc.org/internet-history/brief.html

		Infrastructure Development Level	
		Low	High
Terrorist operating base	Rural	Conventional attacks are simpler; more likely	Cyberterror attacks are useful for destabilizing central government and population centers
	Urban	Cyberterror attacks are useful only for foreign targets (e.g. – multi-national corporation with subsidiary operating in country).	Cyberterror more likely

Table 4-2: Effect of Infrastructure Development on Cyberterror Utility

Unlike in the late 1970s, computer networks today represent a tool for the disaffected to leverage their time to communicate their message to a large public audience, as is evident by the number of homepages for disaffected groups found on the web today.[97] Disruption of this medium, in an unfocused manner, may be counterproductive for revolutionary terrorists. However, focused application of cyberterror in support of traditional revolutionary violence is consistent with revolutionary ideology. In particular, focused attacks against governments and corporations may be highly attractive to revolutionary terrorists.

To summarize, for revolutionary terrorists:

- Attractiveness of cyberterror is primarily related to the information-systems dependency of the adversary, with an added emphasis on the rural/urban context.
- Continued IT use to facilitate propaganda is attractive.
- Simple-unstructured attacks are likely to prove non-coercive.
- Advanced-structured attacks can support continued application of traditional terrorism, and can also be employed in a stand-alone approach against commercial/capitalist interests within the opposed state.

[97] The Anti-Defamation League maintains a list of extremist groups that utilize the Internet. For more information see http://www.adl.org/frames/front_terrorism_up.html.

- Mass disruption is unattractive, because of unfocused effects and the changing symbolization of information systems.

3. Far Right Extremist Terrorism

Within far-right extremist groups[98], "there is usually the idea that certain groups of people are inferior or superior as an innate principle. This is combined with an acceptance of violence as a legitimate form of action."[99] Hatred of socialism or communism and a tendency towards authoritarianism are common traits among far-right extremist groups.[100] These groups vary in their use of violence, but "the most extreme groups, such as the Nazis and modern Italian neo-fascists, see violence as a creative, cleansing force."[101]

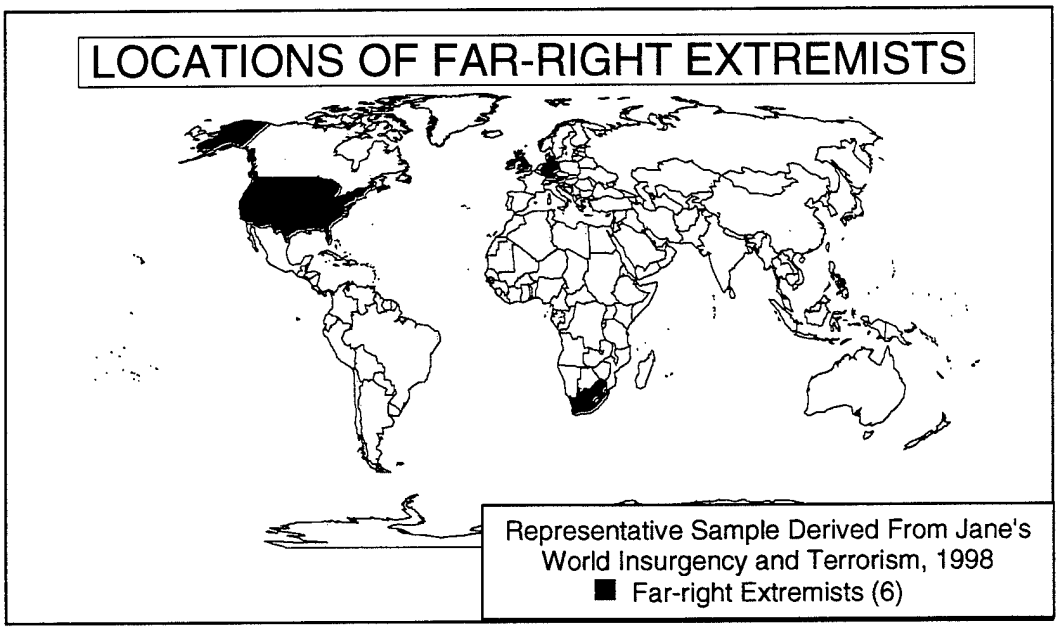


Figure 4-3

Even though right-wing extremists operate within today's advanced information societies (see chapter III), information infrastructure attacks by right-wing terrorists are unlikely because unfocused application of cyberterror would create a large number of collateral victims, some of whom may be

[98] Due to legal constraints, U.S. based extremist groups were not considered by this working group.

[99] Tore Bjorgo, "Far-Right Extremism," *Encyclopedia of World Terrorism,* ed. Martha Crenshaw and John Pimlott (Armonk: M.E. Shapre, 1997), p. 197.

[100] Tore Bjorgo, "Far-Right Extremism," p. 197.

[101] Tore Bjorgo, "Far-Right Extremism," p. 197.

supporters of the extremist cause. With respect to information infrastructure, of all the types of terrorist groups, the right-wing groups have shown the most extensive use of the Internet for propaganda purposes, selling of survivalist gear, and proliferation of hate material.[102] They may therefore be disinclined to attack or disrupt something that they view as an effective tool for their movement.

An essential characteristic of far-right extremism is the psychology involved in the application of their violence. Seeing the enemy as inferior and using violence as a cleansing force provides the extremist satisfaction and reaffirms their self-fulfilling logic of dominance over the inferior group. Cyberterror's lack of personal contact and disconnection from its target are unlikely to satisfy the psychological needs of some far-right extremist groups.

Recognizing these disincentives leads to the following forecast regarding far-right terrorist use of cyberterror:

- Operations will occur in advanced information societies.
- They will continue use of IT for support operations.
- Cyberterror attacks against traditional targets will fail to satisfy the psychological needs of both the group and individual.
- Mass disruption may be unattractive because its effects would often impact the group's own support operations.

4. New Age Terrorism

When the stomach is full, one looks for something else to do.

Chinese proverb

New age terrorist (single-issue) groups turn to violence "when they believe that the issues they promote become too urgent for the slow progress of traditional campaigning."[103] New age terrorist groups, such as anti-abortion and animal rights groups, differ from revolutionary terrorists because new age terrorist groups focus on one issue above all else, where as revolutionary

[102] Post, Ruby, & Shaw, p. 8.

[103] Toby Dodge, "Single-Issue Group Terrorism," *Encyclopedia of World Terrorism,* ed. Martha Crenshaw and John Pimlott (Armonk: M.E. Shapre, 1997), p. 200.

terrorists generally have wider aims. New age terrorist groups are seldom, if ever, found outside the context of a greater single-issue, legal, social movement. The new age terrorist group can, and probably does, act independently from the law-abiding majority of the movement.

New age terrorist acts tend to be focused in nature against particular industries, sections of society, or corporations. The Animal Liberation Front (ALF) initially concentrated on targeting pharmaceutical companies, which used animals for scientific research. The ALF maintains an espoused non-violence strategy against humans, and instead focuses on disrupting company operations in an effort to force them out of business. Past ALF tactics include arson and sabotage.[104] Cyberterror offers these terrorists the ability to target and attack specific corporations via the cyber realm by disruption of E-commerce or web-based advertising. The degree to which the particular corporation is cyber-vulnerable then becomes the relevant variable. Since targeting national level infrastructure is inconsistent with most new age terrorist ideologies,[105] the likelihood of such an event is low. But, cyberterror at the simple-unstructured level would be attractive to the new age terrorist due to its ability to expand the terrorist's target set at a relatively low cost and low level of expertise.

The ALF uses the Internet as a communications medium and to promote their cause.

> The ALF and associated groups maintain a number of web sites posting reports on recent attacks, appealing to users to write to imprisoned members and giving advice on security. Activists also communicate by E-mail.[106]

The ALF operates around the world but most of their terrorist activity takes place within the United Kingdom, Canada, and United States.

---

[104] James, Morris, and Pienaar, *Jane's World Insurgency and Terrorism.* (United Kingdom, Jan 98) "Single Issue Terrorism."

[105] Other animal rights terrorists such as the Animal Rights Militia and Justice Department have expanded their target sets from facilities to the individuals involved in the activity, but still the application of violence has been focused in nature and not indiscriminately applied against society. See James, Morris, and Pienaar, *Jane's World Insurgency and Terrorism.* (United Kingdom, Jan 98) "Single Issue Terrorism."

[106] James, Morris, and Pienaar, *Jane's World Insurgency and Terrorism.* (United Kingdom, Jan 98) "Single Issue Terrorism."

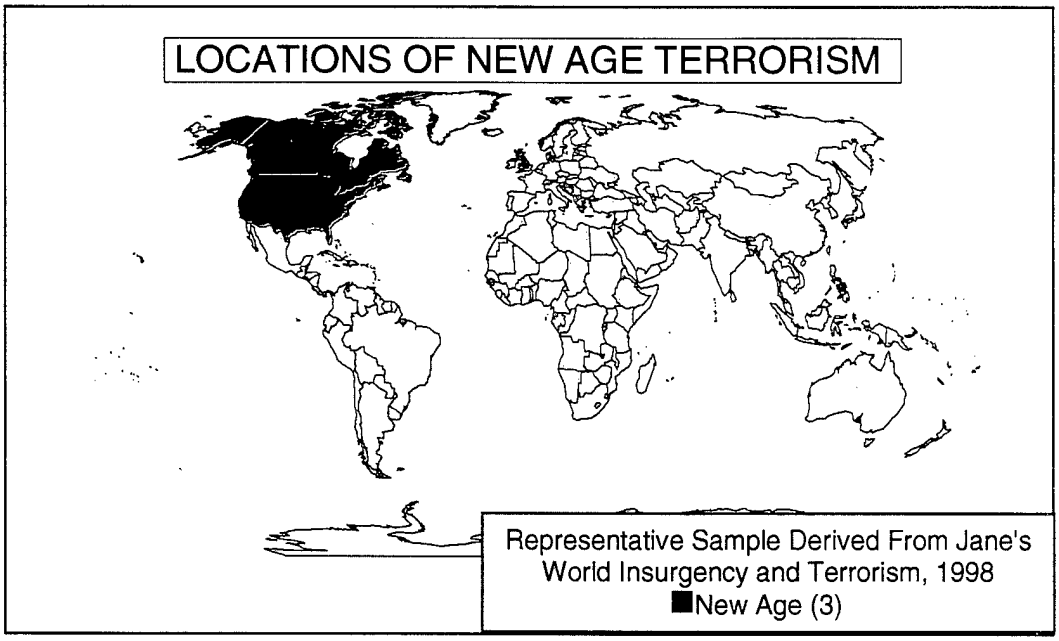


Figure 4-4

> ...the ALF is believed to consist mainly of bright, young, middle class individuals, including computer science students and even some professionals.[107]

Based on these considerations, new age terrorists will likely:

- Operate in advanced information societies.
- Continue use of IT for support operations such as communications and propaganda.
- Find simple-unstructured attacks attractive because they expand their range of 'property' targets at a low cost.
- Develop advanced-structured attacks to provide a greater probability of attack success in disrupting E-commerce of targeted corporations.
- Reject complex-coordinated effects of mass disruption as inconsistent with ideology and past group behavior.

---

[107] James, Morris, and Pienaar, *Jane's World Insurgency and Terrorism*. (United Kingdom, Jan 98) "Single Issue Terrorism."

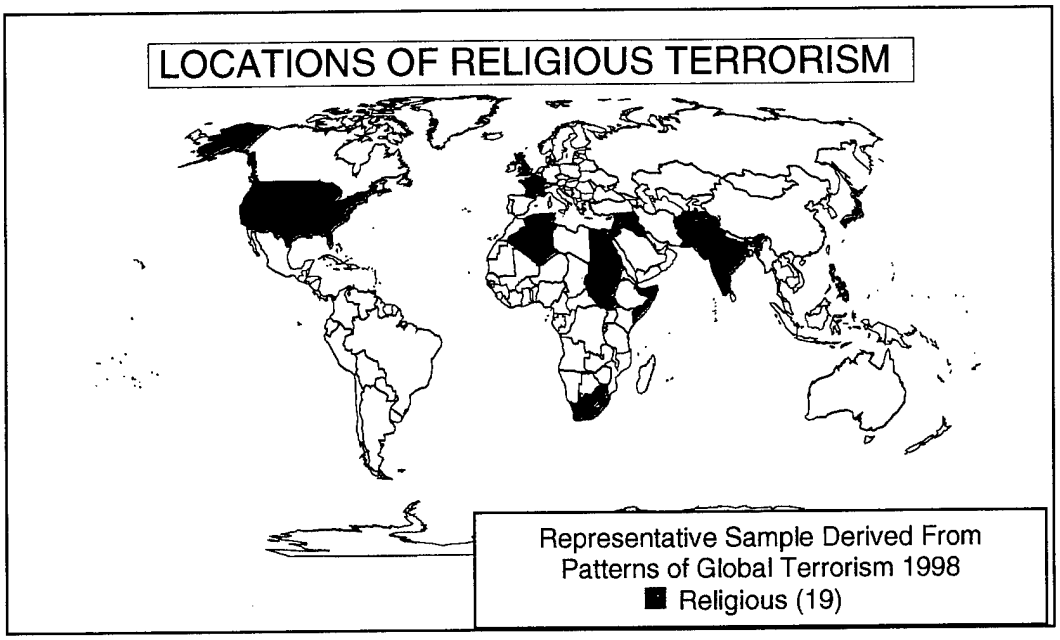


Figure 4-5

5. Religious Terrorism

Religious extremism represents the fastest growing type of terrorism. "In 1968, none of the identifiable active terrorist groups were religious. Today, there are about 50 known groups, and about a quarter of them are religious in motivation."[108] The roots of religious extremism go back over 2,000 years, but for most of the twentieth century, motivations based on ideological issues, such as Marxism or nationalism, have been more prevalent. For the religiously motivated terrorist, "violence is an inspired duty carried out in response to some specific theological belief. So this extremism has a god-driven aspect absent for secular terrorism."[109] Contrary to the revolutionary terrorist's tendency to focus violence, religious extremists "have engaged in more indiscriminate acts of violence, directed against a far wider category of targets encompassing not merely their declared enemies, but anyone who does not share their religious faith."[110] Some of these acts have been designed to require the supreme sacrifice, of the adherent's life. [111]

---

[108] Bruce Hoffman, "Religious Extremism," *Encyclopedia of World Terrorism,* ed. Martha Crenshaw and John Pimlott (Armonk: M.E. Shapre, 1997), p. 210.

[109] Hoffman, "Religious Extremism," p. 210.

[110] Hoffman, *Inside Terrorism,* pp. 158-159.

[111] There is some evidence however that suicide bombers do not represent the group as a whole. Harvey W. Kushner points out that the suicide bombers employed in Israel and the West Bank are specially recruited and trained in isolation from other terrorists. Harvey W. Kushner, "Suicide Bombers: Business as Usual," *Studies in Conflict and Terrorism* 19.4 (Oct-Dec 1996): pp. 329-337.

From the characteristics described above, cyberterror use by the religious terrorist would be ideologically consistent with regard to complex-coordinated cyberterror attacks against targets which may cause mass disruptions – such as information-systems control mechanisms for critical infrastructures. Simple-unstructured attacks, which require little or no self-sacrifice, may be inconsistent with the intrinsic motivations of religious terrorists. To summarize, for religious terrorists:

- IT use to facilitate global expansion is highly attractive.
- Simple-unstructured attacks fail to rise to the level of destruction or violence consistent with religious terrorism.
- Advanced-structured attacks begin to offer the returns consistent with religious terrorism.
- Complex-coordinated attacks are most consistent with ideology and motivations.

6. Hacker groups

The final group we examine is the hacker organization that may wish to cross over into terrorism. Such a group would already have many of the necessary technical skills to perform advanced-structured and possibly even complex-coordinated attacks (see Chapter Five). These factors tend to make hacker groups some of the most menacing from a cyberterror perspective. Indeed, it can be argued that hacker groups are the only organizations known to possess the technical prowess associated with a complex-coordinated capability level. Some hacker groups have used their skills to publicize various causes creating a phenomenon called "hacktivism." Their venom has been directed against targets from Switzerland[112] to China[113].

On closer inspection, the hacker menace appears less threatening. The only verified "hacktivist" strikes have been against worldwide web and mail servers. Although these groups have declared their support for a variety of causes, the only cause that they dependably support is freedom of

[112] Niall McKay, "The Golden Age of Hacktivism," *Wired News*. 22 Sept. 1998. http://www.wired.com

[113] Sumner Lemon, "It's Payback Time, Say Mainland Hackers," *Computerworld Hong Kong* (On-line version). 11 August 1998. http://www.cw.com.hk/Features/f980811001.htm

information.[114] Furthermore, they are loose affiliations whose primary purpose is to provide a forum for the exchange of information and braggadocio. Hacker groups have little to no centralized authority. While they may recognize certain members as particularly skilled, they are resistant to official hierarchy. Group members often remain anonymous to each other and tend toward paranoia. These traits, combined with their "virtual" organizations, inhibit the building of trust.

The individual members themselves tend to be loners. They usually put their own self-interests above those of the group.[115] They have an abysmal record of keeping secrets. When arrested, they have historically been very cooperative.[116] Hackers draw their identity from their mastery of the information infrastructure. The loss of that infrastructure is counter to their self-interest. The group character described above and these individual characteristics make it unlikely that hacker groups will pursue anything beyond the advanced-structured level.

- Technically complex attacks are consistent with the character and ideology of hacker groups; but
- Coordinated attacks are inconsistent with the group dynamics of hacker groups.
- Hacker groups have a stake in the continued availability of the information infrastructure.
- Hackers are likely to continue to make political statements through information technology.

C. Psychological Analysis

A second approach to understanding the "demand side" of cyberterror is to analyze terrorist acts as the result of psychological factors, both individual and

---

[114] One group recently advocated a cyberwar against countries with poor human rights records. Other groups discouraged the action, pointing out the risk to information freedom that would likely result. The initiating group backed down. See the joint hacker group statement at http://www.l0pht.com/lou.html

[115] The only exception has been over freedom of information issues.

[116] See the account of Operation Sundevil in Bruce Sterling, *The Hacker Crackdown: Law and Disorder on the Electronic Frontier* (New York: Bantam Books, 1992).

group.[117] However, understanding the psychology of the individual terrorist is difficult. Aside from the obvious difficulty in observing terrorists in an appropriate setting, this approach also has "serious methodological problems," such as a lack of a control group and the possibility that behavior and motivations are affected by participation in illegal activities.[118]

> Comparative studies of terrorist psychology do not indicate a unique terrorist mind. Terrorists do not fit into a specific psychiatric diagnostic category. Indeed, most would be considered to fit within the spectrum of normality.[119]

Despite the difficulties associated with individual psychological analysis, group psychology can offer valuable insights about decision-making processes in a terrorist organization. [120] In particular, there is a tendency toward a collective reasoning in which individual judgement is suspended in the interest of conforming to group expectations and maintaining a sense of belonging.[121]

A weakness of the group psychology approach is its dependence on an understanding the organizational structure of the terrorist organization. According to Post, "Both structure and social origin are of consequence. Identification of the locus of power and decision-making authority is particularly important to structural analysis."[122] These attributes can be particularly difficult to determine, especially when terrorist organizations adopt a network structure with decentralized decision-making and loose coordination.

---

[117] Jerrold M. Post, "Terrorist Psycho-logic: Terrorist Behavior as a Product of Psychological Forces," *The Origins of Terrorism*, ed. Walter Reich (Washington, D.C.: Woodrow Wilson Center Press, 1990), pp. 25-42.

[118] Crenshaw, "The Causes of Terrorism," p. 391.

[119] Jerrold M. Post, "Prospects for Nuclear Terrorism: Psychological Motivations and Constraints," *Preventing Nuclear Terrorism,* ed. Paul Leventhal and Yonah Alexander (New York: Lexington Books, 1987), p. 92.

[120] Post, "Prospects," p. 93. See also Post, "Terrorist Psycho-Logic," pp. 25-40.

[121] Post, "Prospects," pp. 93-99. See also Jerrold M. Post, "Narcissism and the Charismatic Leader-Follower Relationship," *Political Psychology* 7.4 (1986): pp. 675-687.

[122] Post, "Terrorist Psycho-Logic," p. 32.

1. The Effects of Group Dynamics

The pressure in small groups to conform may pose a barrier to the innovation[123] necessary to implement cyberterror. Implementing an advanced-structured or complex-coordinated cyberterror capability would be a significant innovation for any existing terrorist organization. It would likely involve strategic, structural, and cultural changes within the organization. The dynamics of small groups may make it difficult to overcome the natural resistance to change.

New technologies are usually simply embedded in existing organizational structures without resulting in real innovation.[124] Simple-unstructured level cyberterrorism is an adoption, not truly an innovation; it is the result of the diffusion of IT to terrorist organizations without any structural change. It can be accomplished with little organizational restructuring and simply reflect the same applications of IT that we have seen in legitimate organizations: improved communications, coordination, and efficiency. However, as Chapter Five will show, advanced-structured and complex-coordinated levels are significant departures from past practices, and will likely require a greater level of organizational innovation/restructuring. There is typically a great deal of opposition to restructuring.

---

[123] There are at least two frames of reference for innovation. One is industry-based: "an item is judged to be an innovation if it represents a significant departure from the state of the art in a given field at the time it appears." The other perspective is from the organization; "the item is judged to be a significant departure for the organization." We use the term "innovation" to denote the introduction of a new process or strategy from the perspective of an organization. That is, the particular process or strategy is new to that specific organization. In reality, it may actually be an adaptation or diffusion of somebody else's innovation. John R. Kimberly, "Organizational and Contextual Influences on the Diffusion of Technological Innovation," *New Technology as Organizational Innovation: The Development and Diffusion of Microelectronics,* ed. Johannes M. Pennings and Arend Buitendam (Cambridge: Ballinger, 1987), p. 248.

[124] John Child, Hans-Dieter Ganter and Alfred Kieser, "Technological Innovation and Organizational Conservatism," *New Technology as Organizational Innovation: The Development and Diffusion of Microelectronics,* ed. Johannes M. Pennings and Arend Buitendam (Cambridge: Ballinger, 1987), p. 112.

> Behavioral inertia and organizational conservatism are the norm; rapid and thoroughgoing acceptance of innovation is exceptional. For a variety of reasons, some obvious and some not so obvious, it can be anticipated that most individuals and collectivities will behave in ways that maintain the familiar and screen out the unfamiliar...The probability of innovation's being adopted and used fully is increased to the extent that its visible impact on established routines is relatively small. [125]

Although there are other factors, the role of the "champions," or "boundary spanning individuals" may be one of the most crucial adopter characteristics in the innovation process.[126] Innovation generally requires a "champion," someone with the vision, technological expertise, and credibility to build consensus for change. The innovation decision process generally consists of lower level participants (proponents or "champions") attempting to convince the upper level participants to approve the project. [127] Although it is possible for innovation to be a top down process, it may be more likely to be bottom-up when advanced technology is involved. A study on integrating advanced technology found that lower level technical people are usually responsible for initiating the innovation decision process.

> These individuals are often young, not long out of school, and are fascinated by the potential of advanced technology to improve operations within their company. [128]

Champions generally come in two types: the technical champion and the management champion. The technical champion is the person who "generates or adopts and develops an idea for technological innovation and is

---

[125] Kimberly, p. 238.

[126] Strategic and financial considerations, the credibility and commitment of the "champions," and organizational politics (the ability to generate consensus at lower levels before moving up the chain) influence the process of justification. Other influences are the degree to which adoption and implementation distracts from current operations; the position of the proponents in the organizational structure/hierarchy also affects decision-making.

[127] James W. Dean Jr., "Building the Future: The Justification Process for New Technology," *New Technology as Organizational Innovation: The Development and Diffusion of Microelectronics,* ed. Johannes M. Pennings and Arend Buitendam (Cambridge: Ballinger, 1987), p. 39.

[128] Dean, p. 38.

devoted to it." A management champion "acts as a supporter or sponsor to shield and promote the idea within an organization."[129]

In legitimate organizations, these individuals must build a consensus for change. This will be particularly difficult in terrorist organizations as the dynamic of small groups, particularly in underground organizations, tends to enforce conformity.[130] It may be difficult to voice opinions about even small changes, let alone the radical changes that the advanced-structured and complex-coordinated levels of cyberterror require. An exception may be when an informal group leader becomes the champion. If the champion is not an informal group leader he/she may still influence innovation. The proximity of the champions to the decision-makers also influences the decision.[131] Therefore, the dynamics of small group interactions may inhibit the adoption of cyberterrorism unless a "champion" emerges from the group leadership.

2. Comparison of Individual Motivations

A number of intrinsic and extrinsic motivations may influence an individual to pursue cyberterrorism. The intrinsic motivations are power and self-fulfillment. The extrinsic motivations are pay, non-financial personal benefits, responsibility and empowerment. We address these motivations through a comparison of hackers, terrorists and computer technology professionals.

Hackers and terrorists both are generally young and narcissistic. At a certain level, they also crave attention. They are, to some degree, isolated from other social contacts. Both may be isolated from their families and friends and alienated from society.[132] However, one defining difference is how each chooses to carry out their activities. While both may be considered action-oriented, the terrorist depends upon physical action whereas hacker activities are conducted *virtually* and remotely. Excepting the minority personality that derives satisfaction from both forms, it is unlikely that members of one group will accept the activity of the other, and vice versa.

---

[129] Richard L. Daft, *Organization Theory and Design*, 6th ed. (Cincinnati: South-Western College Publishing, 1998), p. 297. See also Kimberly, p. 248 and James L. McKenney, *Waves of Change: Business Evolution Through Information Technology* (Cambridge: Harvard Business School Press, 1995), p. 210; Peter J. Frost and Carolyn P. Egri, "The Political Process of Innovation," *Research in Organizational Behavior,* Vol. 13 ed. L.L. Cummings and Barry M. Straw (New York: JAI Press, 1991), pp. 229-95; Jay R. Galbraith, "Designing the Innovating Organization," *Organizational Dynamics,* Winter 1982, pp. 5-25.

[130] Post, *Terrorist Psycho-Logic,* pp. 33-34.

[131] Dean, pp. 53-57.

[132] Allen N. Chantler, *Risk: The Profile of the Computer Hacker* (Doctoral Thesis, Curtin University of Technology), pp. 163-166.

Hackers and computer technology professionals have an intrinsic motivation to work with information technology and find dealing with technology a challenge. Computer professionals are currently in great demand yet there is a short supply of qualified specialists. Ironically, hackers (particularly amateurs) are multiplying rapidly given the proliferation of tools available via the Internet. Both share extrinsic motivations from compensation and autonomy, however, only professionals have the ability to find legitimate employment with generous compensation because of shortages of skilled applicants. Many companies are hesitant to hire known hackers given the obvious risks associated with their employment.

While membership in a terrorist organization may at some level provide intrinsic motivation for an individual hacker, or technology professional, it is unlikely to provide much in the way of extrinsic motivations. As previously stated, terrorist organizations typically form around a group's ideological interests first, and later are subordinated to the interests of the individuals in the group. At the group level, interests include overthrowing the state, establishing a new order, or the pursuing a specific ideal such as animal rights. At the individual level, interests range from power to revenge and self-fulfillment. Terrorist groups, limited in resources, generally do not provide monetary incentives to its members. Terrorists groups generally do not empower their members beyond their specific specialties. Unlike the highly trained knowledge workers of today's information technology organizations, terrorist specialists are simply 'highly skilled' at a dangerous, but simple, specialty. IT professionals can demand greater levels of empowerment because of the difficult nature of their skills, whereas terrorist specialists can not.

D. Organizational Analysis

> [A]cts of terrorism may be motivated by the imperative of organizational survival or the requirements of competition with rival terrorist groups. Terrorism is the outcome of the internal dynamics of the organization, a decision-making process that links collectively held values and goals to the perceptions of the environment. An organizational approach assumes that members may be attracted to terrorist organizations as much for nonpolitical as political ends. Incentives to join can include comradeship, social status, excitement, or material reward. The longer a terrorist organization exists, the more likely that group solidarity will replace political purpose as the dominant incentive for members.[133]

A third approach to understanding the "demand" for cyberterror is to examine terrorist acts as the result of organizational processes based on their similarities to other voluntary organizations.[134] An analysis which focuses on organizational processes "assumes a complexity of motivation well beyond the strategy of challenging governments to effect radical change."[135] This approach assumes that terrorist organizations, regardless of their political or ideological aims, endeavor to survive above all else and will take actions based on this organizational imperative.

From this perspective, terrorist acts "may serve internal organizational functions of control, discipline, and morale building within the terrorist group and even become an instrument of rivalry among factions in a resistance movement."[136] As an example of this last point, Crenshaw uses the factional terrorism among Palestinian groups intended to gain influence among other groups rather than influence Israeli public opinion.[137] It is important to emphasize that terrorist acts can serve to advance both external strategic and internal organizational goals. While these purposes are not necessarily contradictory, some authors have argued that over time the strategic goals of

---

[133] Crenshaw, "An Organizational Approach," p. 473. See also James Q. Wilson, *Political Organizations* (New York: Basic Books, 1973).

[134] Crenshaw, "An Organizational Approach," pp. 465-488.

[135] Crenshaw, "An Organizational Approach," p. 487.

[136] Crenshaw, "The Causes of Terrorism," p. 387.

[137] Crenshaw, "The Causes of Terrorism," p. 387.

terrorist organizations are subordinated to internal organizational goals to the detriment of the organization. [138]

Applying an organizational analysis to terrorist organizations entails some special considerations. Terrorist organizations differ from other political organizations in several important respects. First, they are clandestine by nature, which complicates efforts at observing internal organizational processes. Second, the clandestine and conspiratorial nature of terrorism results in an extreme emphasis on solidarity and allegiance to the group rather than the espoused political goals.[139] Third, the illegal nature of terrorist organizations may also place constraints on their ability to recruit personnel. It is important to recognize these differences affect the way that terrorist organizations can respond to changes in their environment and that their responses to a given set of circumstances may differ markedly from the responses of legitimate organizations.

The organizational approach provides for a more comprehensive analysis than either a strategic or a psychological analysis alone. In fact, an organizational analysis subsumes these types of analyses while introducing other factors such as organizational structure, goal conflict and organizational life cycle into the analysis. Similar to the previous psychological analysis, this analytical framework is intentionally general.

1. Organizational Structure

> "An innovative organization is characterized by flexibility, empowered employees, and the absence of rigid work rules" [140]

These are not typically the characteristics of terrorist organizations because of the need for security. However, to integrate advanced-structured or complex-coordinated cyberterror capabilities, these organizational characteristics may be a necessary precondition. These characteristics are significantly influenced by an organization's structure.

---

[138] Charles Lockett, *We Bomb, Therefore We Are: The Evolution of Terrorist Group Life Cycles.* (Thesis, Naval Postgraduate School, Monterey, CA, 1994), p. vi. See also J.K. Zawodny, "Internal Organizational Problems and the Source of Tensions of Terrorist Movements as Catalysts of Violence," *Terrorism: An International Journal* 1:3/4 (1978): pp. 277-285.

[139] Crenshaw, "An Organizational Approach," p. 480. See also Wilson, *Political Organizations,* p. 50 and Post, "Terrorist Psycho-Logic," pp. 33-35.

[140] Daft, p. 294.

Structure influences the location of decision-making within the organization. Organic structures foster innovation; mechanistic structures stifle/inhibit innovation but provide the best structure for efficiently producing routine products. Jenkins, Hoffman, and others have noted the general conservatism of terrorist groups. This is because they are generally mechanistic. The same dilemmas that confront military organizations attempting to adopt networked or organic structures confront terrorist organizations: how low can decision-making be delegated before it has an effect on the ability to accomplish objectives or maintain security? Meaning lower-level members of terrorist organizations are not likely to pursue development of cyber capabilities or conduct attacks when given the opportunity because of the risk to themselves and the organization.

2. Goal Conflict within Organizations

Integrating cyberterror with conventional terrorism in an any group, existing or emerging, has the potential to create intra-group conflicts within the terrorist organization. "Goal incompatibility" is probably the greatest source of conflict within organizations. [141] The achievement of one groups' goals interferes with or contradicts another groups' goals. Currently, the principal goal of cyberterrorism is disruption versus the predominant goal of destruction (whether limited or unlimited) in traditional terrorist organizations. While these objectives may be complementary in principle, they may become opposed as an organization expends the resources necessary to achieve a complex-coordinated or advanced-structured cyberterror capability.

Resource scarcity is a common source of conflict in organizations. Groups must compete for limited resources (money, facilities, human resources, etc.). Resources can symbolize power and influence within an organization; the ability to obtain resources enhances prestige. Competition can lead to conflict between groups/cells within an organization. The power wielded by a particular group can play a significant role in structural change, interdepartmental coordination, leadership/management succession, and resource allocation. If the newly formed cyberterror cell consumes resources but does not produce unambiguous success, it may result in a conflict with more traditional elements of the organization. The best chance for avoiding this type of conflict is if the cyberterror cell has a "champion" or patron that wields enough power within the organization to maintain the flow of resources.

[141] Daft, p. 489.

The level of differentiation and competition for resources will increase as the desired capability increases. Differentiation refers to the variations in "cognitive and emotional orientations in different functional departments"[142]

> Functional specialization requires people with specific education, skills, attitudes, and time horizons. The group norms and values influence behavior. Departments or divisions (cells in terrorist groups) may have different values, attitudes, standards, of behavior. These cultural differences can lead to inter-group conflict within the organization.[143]

We see examples of this specialization in traditional terrorist organizations. Such an example is the differentiation between intelligence and operational cells. Each function has distinct requirements and may attract different types of people. Intelligence analysts may have no desire for combat or confrontation. Another example of this is the integration of terrorist suicide bombers. Recent research conducted by Dr Ariel Merari[144] on Hamas and Islamic Jihad suicide bombings reveals that approximately half of those suicide bombers studied were previously active members of the terrorist organizations. The other half were recruited from the group's support base after being identified as willing to pursue martyrdom. Following recruitment, the future bombers were exposed to the religious heads of the organization, trained for their task, and in some cases then secluded from the rest of the group for the week prior to suicide attack. Terrorist bomb-makers provide another data point when examining specialization.

> Skilled bomb-makers are rare in most terrorist organizations. They have invariably had to learn from experience, and many have been killed by their own mistakes. Within a terrorist organization, a distinction is often made between the bombmaker, who never goes near a target and whose skills are carefully preserved, and the other operatives who risk arrest and premature detonations while planting the devices.[145]

Another potential source of conflict is the interdependence between cyberterror cells and conventional operations cells. Interdependence can increase the level of conflict between groups, particularly if it is a reciprocal or

---

[142] Daft, p. 93.

[143] Daft, p. 490.

[144] Dr Ariel Merari was interviewed by phone on 26 July 1999. Dr Merari is a Senior Fellow at the Belfer Center for Science and International Affairs, Kennedy School of Government, Harvard University.

[145] Donald Sommerville, "Bombing Operations," *Encyclopedia of World Terrorism,* ed. Crenshaw and Pimlott (Armonk: M.E. Sharpe, 1997), p. 217.

sequential interdependence.[146] At the advanced-structured and complex-coordinated levels, with cyberterror in a support role for conventional terrorism, interdependence may be either sequential or reciprocal. If the cyberterror capability is unreliable (e.g. – unable to guarantee that a portion of the public switched network will be taken down at a particular time and kept down for a specified period), it may cause tensions with the supported cells. This problem would become particularly acute if the cyberterror cell failed to accomplish a mission that led to the failure (compromise, capture, or death) of members of another cell.

3. The Effects of Organizational Life Cycle

When considering organizational change and innovation the concept of an organizational life cycle provides a useful framework. This concept suggests that organizations "follow a fairly predictable pattern" of sequential stages of organizational development.[147] The developmental stage of an organization is considered a significant determinant of organizational behavior.[148] While this concept has been principally applied to business organizations, there is very little existing research that applies this type of analysis to terrorist organizations. If terrorist organizations do indeed progress through these developmental stages, or similar ones, there are several implications for their ability and willingness to adopt cyberterror. In general, existing terrorist organizations would seem unlikely to adopt radical changes in their *modus operandi*. However, newly formed or emerging terrorist groups may be willing to adopt cyberterror if it is perceived to satisfy their strategic goals.

Recent work on organizational life-cycles suggests that there are four major stages of organizational development: entrepreneurial, collectivity, formalization, and elaboration. A fifth stage (decline) is possible for organizations that fail to adapt to the changing environment. Measuring the lifecycle of underground organizations is difficult.[149] The clandestine nature of terrorist organizations will likely frustrate most attempts to measure the critical

---

[146] Sequential interdependence means that one group relies on the output of another group to complete its work. Reciprocal interdependence means that the groups mutually exchange information and products.

[147] Daft, pp. 173-185. See also Robert E. Quinn and Kim Cameron, "Organizational Life Cycles and Shifting Criteria for Effectiveness: Some Preliminary Evidence," *Management Science* 29 (1983): pp. 33-51; and Larry E. Grenier, "Evolution and Revolution as Organizations Grow," *Harvard Business Review* 50 (July-August 1972): pp. 37-46.

[148] For business-oriented organizations, there are several indicators of lifecycle stage: organizational structure, management style and systems, goals, reward/control systems, and the variety of products or services. Daft, p. 178.

[149] Martha Crenshaw, "How Terrorism Declines," *Terrorism and Political Violence*, 3.1 (Spring 1991): pp. 69-87.

indicators such as organizational size, structure, resources, etc. However, as a starting point for further analysis, we introduce this life cycle framework.

Table 4-3 summarizes the major characteristics of each stage.

Stage	Characteristics
Entrepreneurial	Informal; non-bureaucratic; ambiguous goals; high creativity.
Collectivity	Hierarchy of authority begins to develop but structure and communication are informal; high commitment to the organization.
Formalization	Increased bureaucracy; formalization of rules, structure and incentives. Emphasis on efficiency, characterized by division of labor. Innovation may be restricted.
Elaboration	More complex structure; decentralization; diversified products/services. Organization may become too bureaucratized to respond to changes in the environment.
Decline	Failure to adapt to environment causes decline in competitiveness and profit leading to conflict, dissention; high employee turnover rate.

Table 4-3: Stage Characteristics[150]

It is important to note that not every organization reaches the decline stage. Effective responses to changes in the environment can allow continued productivity and organizational viability. Still others organizations may attempt to maintain themselves at a specific stage. For example, at one time the management of Apple Computer made an explicit commitment to try to remain in the collectivity stage for as long as possible. [151] It is also important to emphasize that the age of an organization does not necessarily correlate with any specific developmental stage; organizations will develop at different rates.[152] The overall size is not necessarily an indicator of a developmental stages either; it is possible for small organizations to become rigid and bureaucratic.

[150] Adapted from Daft, esp. pp. 173-185.

[151] Stephen P. Robbins, *Organization Theory: Structure, Design and Applications,* 2d ed. (Englewood Cliffs: Prentice-Hall, 1987), p. 18.

[152] Robbins, p. 18.

Both organizational and individual security relies explicitly on formal rules and procedures to prevent compromise.[153] Because terrorist organizations have an inherent need for secrecy to protect them, they must rapidly reach the formalization stage. It is at this stage that formal structure and rules are implemented. It is also at this stage that innovation can become more difficult as efficiency and stability are emphasized.[154] Therefore, terrorist organizations at this stage of development may be unlikely to innovate[155] voluntarily as long as they perceive their current tactics as successful. However, competition from other terrorist groups or effective countermeasures by security forces can create incentives to innovate. Still, the majority of terrorist groups have not demonstrated a willingness to undertake the type of radical transformations that would be necessary to implement an advanced-structured cyberterror capability.

> However radical or revolutionary these (radical leftist and ethno-nationalist) groups were politically, the vast majority were equally conservative in their operations. These types of terrorists were said to be demonstrably more 'imitative than innovative', having a very limited tactical repertoire directed against a similarly narrow target set. They were judged as hesitant to take advantage of new situations, let alone create new opportunities. [156]

The innovations by terrorist organizations came principally in the choice of targets and method to conceal or detonate bombs; they still employed hijackings, bombings, and assassinations as their primary tactics.[157] Hoffman believes that the religious and millenarian groups are less constrained than "traditional" terrorists, and therefore more likely to pursue more destructive

---

[153] According to J. Bowyer Bell, the constraints placed on underground organizations for secrecy create an inherently inefficient organization. Advances in information technology, such as cryptography, can mitigate some of the inefficiencies. Indeed, it appears that many terrorist organizations are doing this. Although Bell's article concerns insurgent organizations, the requirements imposed by clandestine operations are equally applicable to terrorist organizations. J. Bowyer Bell, "Aspects of the Dragonworld: Covert Communications and the Rebel Ecosystem," *International Journal of Intelligence and Counterintelligence* 3.1 (Spring 1989): pp. 15-43.

[154] Robbins, p. 17.

[155] Innovation has a variety of definitions. In the broadest sense, it means simply to introduce something new. For our purposes, we have adopted the definition offered by Arquilla, et. al., "Innovation is manifested by the development of new warfighting concepts and/or new means of integrating technology. New means of integrating technology might include revised doctrine, tactics, training, or support." See Jeffrey Isaacson, John Arquilla, and Christopher Layne, *Predicting Military Innovation* (Santa Monica: RAND, 1999), p. 8.

[156] Hoffman, *Inside Terrorism,* p. 198. The quote is from Brian Michael Jenkins, *International Terrorism: The Other World War* (Santa Monica: RAND, 1985), p. 12.

[157] Hoffman, *Inside Terrorism,* p. 198.

means.[158] Assuming these groups accept mass disruption as a suitable substitute for destruction, we may conclude that these types of groups, as we have argued earlier, are likely to pursue advanced-structured and complex-coordinated cyberterror capabilities.

Life cycle theory predicts that organizations in the elaboration phase will search for "new products and growth opportunities."[159] However, innovation at this stage is generally accomplished through institutionalized research and development. Terrorist organizations are typically limited in their resources and, unlike business organizations, may not actively seek growth opportunities. Further, even if they did pursue innovation, it is unclear whether they would seek radical change at this stage of development.

While existing terrorist organizations may be hesitant to innovate, emerging terrorist groups may be likely to innovate (at least with regards to contemporary terrorism). Life cycle theory predicts that emerging organizations in the entrepreneurial and collectivity stages are highly creative. These immature organizations have few of the restrictions that can potentially retard innovation in more mature organizations. They are already assuming a large risk by establishing a new organization. They may therefore be willing to attempt innovative tactics with theoretical, but unproven, utility. This willingness to take risks could also apply to splinter groups from existing organizations.

E. Summary

Is there a demand side for cyberterrorism?

This chapter highlighted those terrorist organizations which are likely to take advantage of the opportunities made available by the information age. This analysis, what we refer to as the demand side of cyberterrorism, took into account terrorist ideology and group and individual psychological interests.

From the individual and group psychological perspective we make the following observations.

- Advanced-structured and complex-coordinated cyberterror capabilities require innovation and/or restructuring at the organizational level.

---

[158] Hoffman, *Inside Terrorism,* pp. 196-205.

[159] Robbins, p. 17.

- Terrorist organizations are typically opposed to restructuring.
- Pressure to conform is a barrier to innovation.
- Opposition to innovation may be offset by a "champion."
- Innovation is more likely to develop from the bottom-up rather than the top-down.

From the strategic perspective, we synthesize both the supply and demand sides of cyberterror to reach 'equilibrium' results.

- It is probable that new age terrorists will desire their 'best-fit' cyberterror capability (see figure 4-6 for 'best fits').
- It is possible that ENS, revolutionary, and religious terrorist have the necessary incentives to pursue their respective 'best fit' capability.
- It is unlikely that far-right extremists will desire cyberterror.
- Hackers are unlikely to cross over to cyberterror.

The likely capability level results are summarized in figure 4-6.

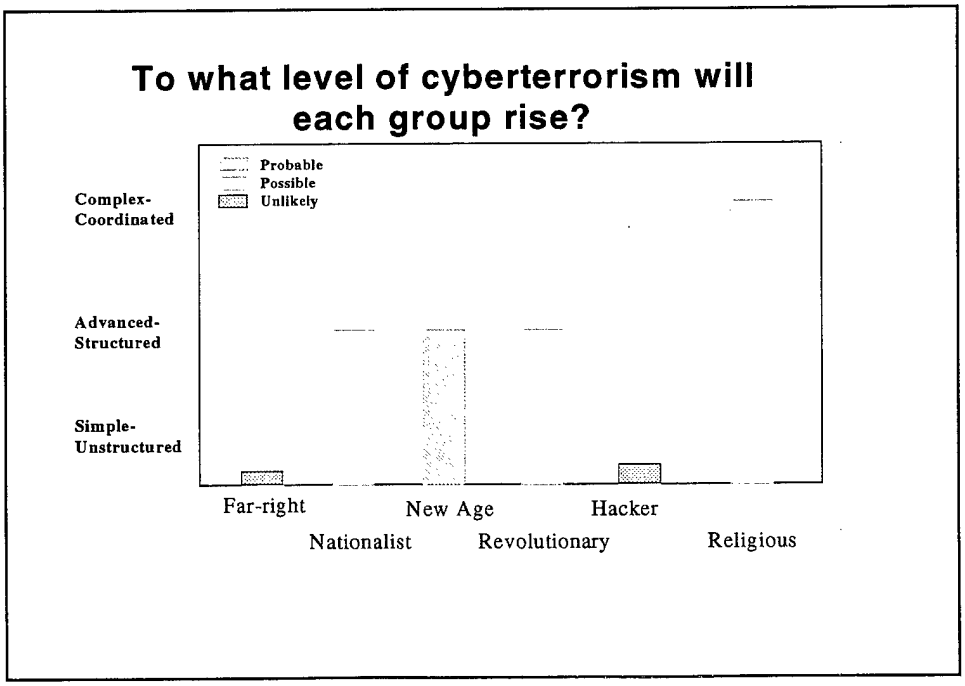


Figure 4-6: "Best Fit" Levels of Cyberterror

In sum, most terrorists will seek at least an advanced-structured cyberterror capability; but only religious terrorists will have incentives to develop complex-coordinated capabilities. To the extent to which the other types of terrorist groups have some religious motivations, this finding could be very troubling.

V. Capabilities and Resources - What is Necessary for Cyberterrorism?

> It is not good to have zeal without knowledge, nor to be hasty and miss the way.
>
> -- Proverbs 19:2 (NIV Translation)

In previous chapters we identified the factors that might encourage or discourage the pursuit of cyberterrorism from the environmental and organizational perspectives. In this chapter we turn to the detailed skill components that constitute a given capability level. This material should provide a better understanding of the obstacles placed before an organization that wishes to pursue cyberterrorism. Combining this information with that provided previously enables an assessment as to whether terrorists can move effectively into the cyber realm.

A. Introduction

The ability to wage cyberterrorism depends on more than technical savvy. It requires a combination of technical, analytical and organizational talents. A cyberterror organization will hold a mix of these skills, in varying proportions. Although a group cannot be utterly devoid of any particular skill, it is the group's aggregate capability that matters. We believe that a group's capability level is the equally-weighted average of its individual skill levels.

Figure 5-1 provides a graphic depiction of two possible variations in composition for a capability level. The first set of columns depicts a successful, established terrorist group that is building its technical skills. They have a well-developed command and control system and intelligence gathering capability. This propels them into the advanced-structured capability level even though their technical skills are not yet at that level. In contrast, the second set of columns depicts a hacker group that decided to pursue a terrorist agenda. In this case, the group has technical skills sufficient for a complex-coordinated capability but lacks the command and control system to achieve their full potential.

Structuring the capability levels this way would seem to allow the possibility of combinations such as a "complex-unstructured" capability. While such combinations are theoretically possible, our working hypothesis has been that growth in ability to mount attacks of increasing complexity parallels the growth in technical skill. We base this on two facts. The first is that the utility of cyberterrorism depends on both the quality of the attack tools and the

precision with which they are applied. The second is that both target analysis and real-time command and control capabilities are at least partially dependent on technical skill.

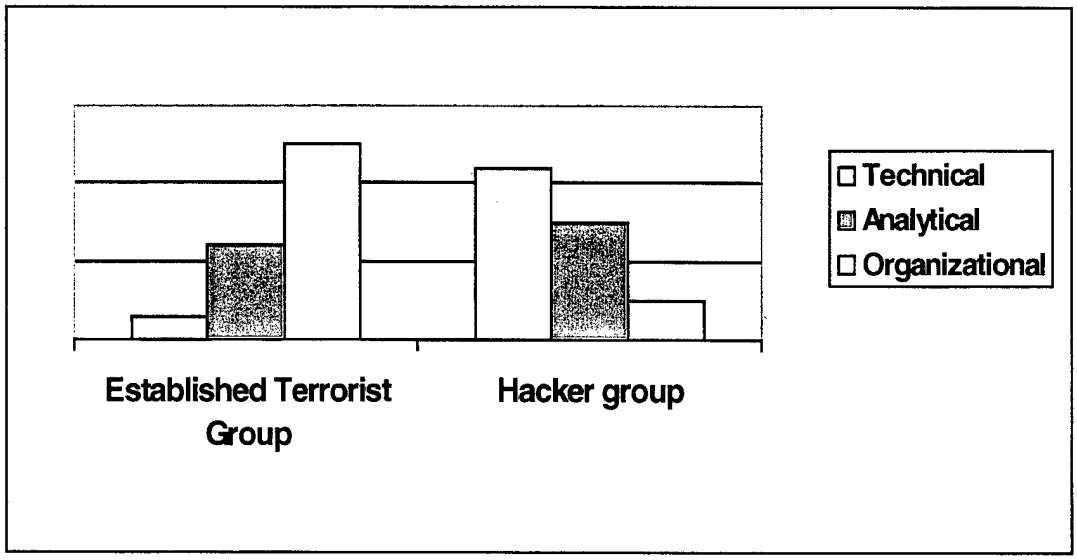


Figure 5-1: Skill Composition Comparison

A given skill level does not imply an inherent cap on destructive potential. An unskilled attacker could stumble upon a critical vulnerability that produces substantial cascading effects. However, a terrorist group depending on such a "lucky shot" would be foolish.

> For example, component failures are a certainty, but the probability that the loss of a single transformer, switching device, or sensor, for example, would trigger a chain reaction that disrupts a major portion of the network (although it does happen) is usually quite small.[160]

In Chapter Two, we defined the distinction between cyberterror support activity and direct attacks. The crux of that distinction was whether the terrorist deed was intended to have a coercive effect. We believe that this distinction holds across the three capability levels. Any level of capability can be used for either support activity or as a primary means of attack. The fundamental difference between cyberterror support and cyberterror attacks with regard to capability level lies in the incentives to seek increasing capability. As we shall see, the higher capability levels place significant demands on an organization. A cost-benefit analysis will not favor pursuit of higher capability levels solely for support purposes.

---

[160] The White House, Office of the Science and Technology Advisor, *Cybernation: The American Infrastructure in the Information Age* (Washington, D.C.: GPO, 1996), p. 21.

B. Defining the Components of the Capability Levels

The technical expertise requirements include knowledge of the characteristics (both hardware and software) of each of the nodes on the path from the attacker to the ultimate objective. These nodes include the terrorists' own cyberterror resources (i.e. programs), the target's resources and those of any intervening network. The technical requirements become more burdensome as the variety and complexity of the nodes increases.

The required analytical skills center around conducting a detailed nodal analysis of a candidate target. This analysis should result in the identification of vulnerabilities and inter-nodal dependencies. Ultimately the terrorist must determine the critical nodes and how those nodes may be attacked. Clearly, a strong technical base is essential for target analysis, but analytical ability goes beyond the technical. Analytical ability is heavily dependent on the intangible qualities of insight and creativity. These qualities are innate talents that some individuals and groups may never possess.

Finally, the organizational capabilities of a group are built on their command and control and group learning talents. A robust command and control system allows the terrorist group to bring its forces to bear at the decisive time and place. Command and control includes both planning and execution. Organizational (or group) learning refers to the ability of the organization to keep pace with new technology and assimilate that technology into their tactics and techniques. This requires the terrorist group to develop an internal mechanism to facilitate the diffusion of knowledge throughout the organization. The group must also conduct sustainment training for their technical specialists.

C. Detailed Analysis

Having defined the three major components of cyberterror capability (technical, analytical and organizational skills), we turn now to a detailed discussion of their respective sub-components. These individual elements of the three components represent the specific barriers to entry for a group pursuing cyberterrorism. Those barriers become formidable as the desired capability level increases.

1. Simple-Unstructured

The capability to conduct basic hacks against individual systems using tools created by someone else. The organization possesses little target analysis, command and control or learning capability.

The simple-unstructured cyberterror capability represents an ability to disrupt individual systems through simple hacks using software tools and techniques created by others. It is estimated that up to 95% of the hacker population resides at this skill level.[161] This level of capability will probably confine an organization to using cyberterror as a supporting activity. An example of cyberterror support at this level would be an ICMP flood (Smurf[162]) attack against all government agencies in the area surrounding a kinetic strike.

If actual cyberterror attacks are conducted at this level, they will likely need to be crafted to create the illusion of greater effect. For example, any successful cyberterror attack on a facility associated with weapons of mass destruction, regardless of actual physical effects, could cause sufficient terror among the populace.

It requires virtually no skill to begin a simple-unstructured cyberterror capability. The only substantial technical skill requirement at this level is knowledge about (and possession of) a UNIX-based operating system. Although it is possible to conduct attacks from a Windows-based platform, an organization choosing to do so has severely limited itself.[163] Beyond that, a group at this skill level will possess the basic computer skills shared by most personal computer owners. This expertise boils down to downloading tools and concomitant instructional material. These groups can issue simple commands and run pre-compiled programs.[164]

The entire body of technical knowledge for a group at this level can reside in one individual. Novices will seek experience by borrowing the tools and techniques from outside sources and use what they acquire to test the waters on their own. Web pages and chat rooms provide an ample source of material, programs, and connections to experienced hackers who can provide mentoring.[165] Once connected, novices can download the programs they need and discuss execution techniques with active hackers.

---

[161] Peter Tippett, quoted in Michael E. Ruane, "New Technology Makes Hacking a Snap," *Washington Post*, 10 Mar. 1999, p. A-1. This statement was confirmed by separate correspondence with Mr. Tippett's executive assistant.

[162] The hacker program Smurf causes an unwitting site to flood the victim site with Internet Control Message Protocol (ICMP) Echo Replies. The volume of these messages chokes out legitimate traffic. In this scenario, responding agencies would be unable to use computer networks to coordinate their response or to communicate information.

[163] Windows-based systems to not support the manipulation of raw network data to the extent that UNIX-based systems do. They also require specially written drivers to use a sniffer.

[164] The alternative to pre-compiled programs is source code. The use of source code requires a compiler and the knowledge of its use.

[165] Chantler, pp. 156-159.

A key discriminator at this level is that the attackers are largely ignorant of the complexity of the tools they employ.[166] Hacker activity throughout the world has shown us that this is not a null capability. The attackers may not understand authentication and identification security mechanisms, but they can still download and run password cracking programs. Similar examples include the use of worms or viruses.[167]

When organizations at this level gather intelligence for cyberterror, they attempt to find targets to match the tools that they have collected. They look for systems that are either unmistakably open or accessible by tools that the attackers have procured.

The greatest constraint on target intelligence analysis at the simple-unstructured level is the organization's inability to understand the complexities of system level targets. Organizations at this level do not understand the intersystem dependencies or the strategic effects of their activities. The lack of target intelligence in these groups is partially mitigated by the fact that the expertise needed to access the target is contained within the tool and not the user.

> The Task Force agrees that it is easy for skilled individuals (or less skilled people with suitable automated tools) to break into unprotected and poorly configured networked computers and to steal files, install malicious software, or cause a denial of service. However, it is very much more difficult to collect the intelligence needed and to analyze the designs of complex systems so that an attacker could mount an attack that would cause nation-disrupting or war-ending damage at the time and place and for the duration of the attacker's choosing.[168]

The command and control requirements of an organization at this level are minimal with respect to cyberterrorism. Groups at this skill level define success as any negative impact on a chosen target. Simple-unstructured attacks are performed by a single individual or at most a small number of individuals. At this cyberterror capability level, the organization does not retain the necessary technical knowledge to reliably forecast second- and third-order effects. They can identify the immediate effects (i.e. "the server is down") but not the larger technical implications.

---

[166] Director of Central Intelligence (DCI), Scientific and Technical Intelligence Committee, *Proceedings From the Carnegie Mellon Workshop on Network Security STIC 97-001* (Springfield, VA: National Technical Information Service, 1997), p. iii.

[167] Chantler, pp. 84-88.

[168] Defense Science Board, *Report on Information Warfare Defense* (Washington, D.C.: GPO, 1996), p. 2-4.

Although a group could begin using these hacker tools immediately upon downloading them, we believe that terrorists will allow themselves time to become comfortable with the technology. A terrorist group starting out with no computer background can reasonably be expected to take up to six months before feeling comfortable enough to use cyberterror tools in an actual operation.[169]

The disadvantages of remaining at this level are two-fold. First, the ability to do meaningful damage is almost non-existent. Second, attackers with only this level of skill face a substantial risk of failure and compromise.

> These less sophisticated hackers ... are easier to detect and eradicate than educated ones because of standardized behavior and because they do not have experience to know when to abort a hacking attempt and often make repeated attempts at re-entry.[170]

The majority of computer security incidents are facilitated by poor security practices. Victimized organizations often felt that they had nothing worth the effort to protect. Organizations that have identified themselves (or been identified externally) as having critical assets are likely to take greater precautions. From the terrorist perspective, there is substantial risk that as awareness of the threat grows, opportunities against even non-critical sites will decrease. While the hacker community can certainly be counted on to continually develop new means of attacking sites, the terrorist group that wishes to pursue an independent capability must rise to the advanced-structured level at a minimum.

2. Advanced-Structured

The capability to conduct more sophisticated attacks against multiple systems or networks and possibly, to modify or create basic hacking tools. The organization possesses an elementary target analysis capability and command and control structure for sequential attacks from a single location. Some learning ability - can assimilate some new technologies and train personnel.

To rise above the limitations of a simple-unstructured capability, terrorists may wish to pursue an advanced-structured capability. Cyberterrorists at this level

---

[169] All of the development times identified in this paper have been checked by various domain experts and borne out by the academic and professional experiences of the authors.

[170] NetSolve Inc., *ProWatch Secure Network Security Survey (May-September 1997).* Posted to the Bugtraq mailing list 19 Nov 1997 by Craig H. Rowland of Wheelgroup. http://www.securityfocus.com

are equivalent to what the CERT®/CC[171] termed "sophisticates". By their estimation an attacker "with a B.S. or M.S. in Computer Science has more than enough knowledge" to operate at this level "especially, if he or she is knowledgeable about operating systems."[172] This is the level where cyberterror attack becomes realistic as a primary method of attack. A cyberterror organization wishing to pursue this capability cannot be wholly dependent on the Internet for its tools. They must have specially adapted (or developed) tools.

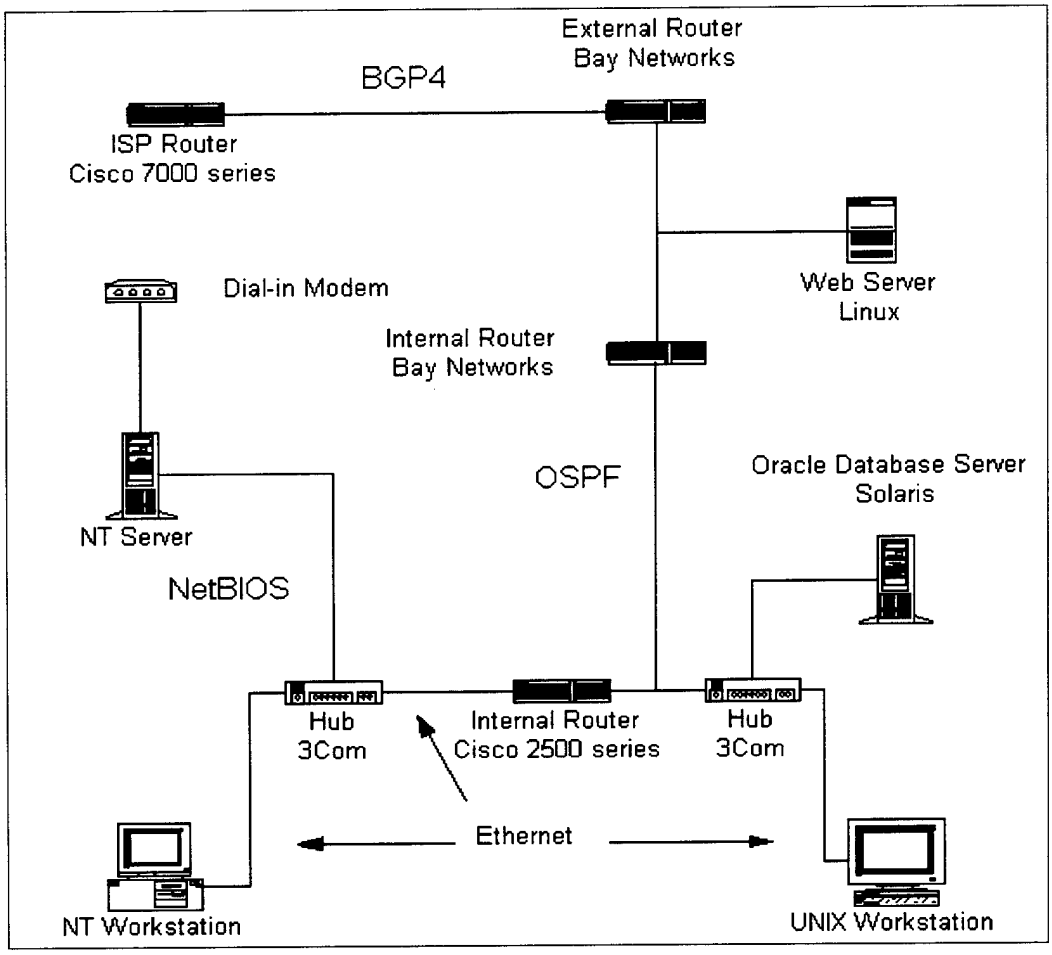


Figure 5-2: Example Heterogeneous Network

At this level, the barriers to entry become more formidable. Technical expertise at this level goes beyond an academic understanding of

[171] The CERT®/CC began as the Computer Emergency Response Team under a government charter in Jan. 1988. It was formed as a result of the Robert Morris Internet Worm incident. Carnegie-Mellon University subsequently registered the term CERT as their trademark title.

[172] DCI, p. 2.

programming principles. An attacker at the advanced-structured level has developed practical knowledge through experience or close personal mentoring. This requirement for 'applied' technical expertise creates a substantial barrier to advanced-structured cyberterror attack even when attacking homogeneous networks or systems. This barrier grows substantially if the group attempts to target heterogeneous networks — those using multiple, proprietary, software, hardware, and firmware components. Figure 5-2 depicts a typical local area network. One can see that even in this small example there are a number of different operating systems, protocols and equipment brands in use.

The required technical knowledge to operate at this level is summarized in Table 5-1. While it is not the full computer science curriculum called for above, it represents a substantial leap from the unskilled computer user at the simple-unstructured level. The knowledge represented at this level empowers a group to defeat a single layer of indirection such as a firewall.

• Sophisticated programming skills.	• Mastery of at least one Operating System.
• Understanding of the mechanics of common security measures.	• Detailed understanding of network & computer architectures.
• Detailed understanding of the TCP/IP protocol suite.	• Familiarity with telecommunications systems & databases.

Table 5-1: Advanced-structured Capability IT Expertise Requirements

The foremost skill requirement is programming expertise. Attackers at this level modify programs or even create small programs of their own. These attackers should have skills in programming for both stand-alone and networked systems. The programming requirement differs from that normally taught in computer science curricula. In order to modify attacks taken from hacker sites, the attacker must be capable of reading a program and following the flow of execution like a storybook. Commercial competition has eliminated some proprietary programming and promoted an environment with standard program functions for interoperability between programs and operating systems. Nonetheless there are subtle variations in execution between operating systems. The advanced-structured level attacker must understand the implications of those variations.

The programmer's language repertoire absolutely must include C or C++.[173] If the attacker cannot program in traditional C (as opposed to C++) he must at least read and understand it. C and C++ are the languages used by the vast majority of hacker tools. They offer the most direct interface with the essential Application Programming Interfaces (APIs) since most operating systems are written in C. The API is the controlling mechanism between application programs and the operating system or the network protocols.[174] Skillful manipulation of the API can give the attacker access to the target system.[175]

Not all of the hacker tools are compiled programs. Many of them are command scripts.[176] As such, the ability to read scripting languages such as Perl and Tcl/tk as well as the traditional OS scripts is essential.

If the terrorist group hopes either to target or utilize worldwide web assets, it must also have the ability to read hypertext mark-up language (HTML) and Java. Java is used widely on the World Wide Web and provides an additional means of attack via what are known as hostile applets. Java applets are small programs that are transmitted with a web page and run locally on the receiver's computer. In addition to hostile applets, a Java-savvy attacker could create elaborate false web pages to collect or hide information.[177]

An individual wishing to become a cyberterrorist should plan on a minimum of six months to meet these programming skill requirements. This six-month figure is based on an academic semester of intense study. Any outside demands on the student's time will only serve to lengthen the required period of study.

Because the performance of most programming languages is dependent on the operating system on which it is compiled, a terrorist with the requisite programming skill will have some knowledge of at least one operating system.

---

[173] C is a 'high-level' programming language designed for systems programming. It is extremely powerful but it uses a cryptic syntax and numerous shortcuts which make it difficult to read. C++ is an object-oriented extension of C.

[174] Douglas E. Comer, *Computer Networks and Internets* (Upper Saddle River, NJ: Prentice Hall, 1997), pp. 285-286.

[175] For example the hacker program *GetAdmin* exploited an API call in Windows NT to give any user administrator privileges.

[176] A command script is similar in function to a program but it consists of a text file containing a series of operating system instructions. They are normally used to automate repetitive tasks. The Autoexec.bat file in MS-DOS is an example of a script. Scripts are used heavily in UNIX environments.

[177] For a detailed discussion of deception using Java see Edward Felton, "Web Spoofing, An Internet Con Game," *Proceedings of the 20th National Information Systems Security Conference, Volume 1* (Baltimore, MD: National Institute of Standards and Technology, 1997), pp. 95-103.

However, to manipulate operating system programs or bypass security measures, his knowledge must go deeper. At a minimum, he should have a detailed understanding of the following topics.

- The file system.
- The identification and authentication (logon) system.
- User and group permissions.
- The auditing and logging system.
- Process execution.
- Input-output (I/O) and inter-process communication handling.

An appreciation of these topics is essential to understanding and exploiting system vulnerabilities.

One of the most ubiquitous computer vulnerabilities is the buffer overflow.[178] Buffer overflows occur when the size of an input item exceeds the size of the memory space allocated to hold it. As a result, the excess input overwrites the contents of the adjacent memory. Buffer overflows often result in denial of service. If operating system code was located adjacent to the overflow, it is possible for well-crafted input to execute system commands. Buffer overflow vulnerabilities are found in operating systems and applications alike. They are very difficult to work with and their effects depend on obscure details of the target system.[179] The majority of root[180] compromise attacks are buffer overflows.[181] Writing a buffer overflow involves direct manipulation of the bits and bytes in the target system's memory. As such, the writer is required to perform binary and hexadecimal math.[182] The writer is similarly required to understand the system architecture and assembly language for his chosen

[178] Of the 50 CERT®/CC advisories published between Jan. 1997 and July 1999, 28 involved buffer overflows.

[179] For a detailed discussion see Aleph One, "Smashing The Stack For Fun and Profit," *Phrack* 7.49 (Nov. 1996). http://www.phrack.com/archive.html

[180] Root, also called administrator, privilege allows full control of a computer.

[181] Based on a survey of the attacks found at the hacker site Fyodor's Playhouse (www.insecure.org). Of the 16 attacks that might allow root privileges, 9 were buffer overflows, 3 were CGI errors, 2 were backdoors, one was a symbolic link error and 1 was not defined. Similar results were obtained using the CERT®/CC advisory data.

[182] This skill is also necessary for working with raw sockets.

target (or targets). Without such an understanding the attacker cannot be sure that the operating system will execute the overflow contents as intended.

Moving outward from the individual host, the next field an attacker must master is Local Area Networks (LANs). A detailed understanding of protocols and topologies enables the cyberterrorist to better identify useful targets and their vulnerabilities. Attacks designed for one protocol or topology often will not work on another. For example, it is possible to install a sniffer[183] via a Trojan Horse. However, most sniffers are designed to work on Ethernet[184] LANs. If the intended victim is on a non-Ethernet (e.g. token-ring) LAN, the sniffer will not work. If it is an Ethernet LAN but it uses switches instead of hubs,[185] the sniffer may not capture anything useful.

At the wide area network level, there are still more protocols and architectures to consider. A detailed understanding of the TCP/IP protocol suite is required for launching advanced attacks across the Internet. This includes knowledge of Classless Inter-Domain Routing (CIDR) and sub-net masking.[186] Without this knowledge an attacker cannot interpret Internet Protocol (IP) addresses and correctly map them to hosts. With this knowledge an attacker can identify and exploit some common addressing practices.[187]

The telecommunications system transmits data across wide areas. It is the backbone of all worldwide electronic connectivity. Familiarity with telecommunications systems enables a group to perform signal interception or denial against open systems. Similar attacks are possible against wireless communications in local and metropolitan area networks. Many SCADA systems use wireless communications with isolated remote terminal units (RTUs).

Taking a broader, system view, an attacker should understand the functioning of common security measures such as firewalls and intrusion detection

---

[183] A sniffer is a program that collects all of the information that passes on the LAN segment to which it is attached. It amounts to a computerized version of a phone tap.

[184] Ethernet is Xerox Corporation's trademarked name for a popular commercial LAN implementation. It uses a broadcast transmission method on a shared medium thus all users can potentially view each other's communications. The term has come to refer to all LANs that use the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocols.

[185] Hubs simply provide a central connection point. Switches direct traffic to individual hosts. This prevents the eavesdropping possible with hubs.

[186] CIDR is a technique for using two or more Class C addresses as if they were a single address. Sometimes referred to as *supernetting*. Subnetting is a technique for hierarchically dividing a site's assigned addresses among smaller sub-networks.

[187] For example, the servers for a given sub-net are usually assigned the low numbers in an address block. What these low numbers are depends on the sub-netting scheme.

systems. These provide the first level of defense against hostile activity against a system or network. Here there are different degrees of firewall protection. Static firewalls check access against an access controls list to grant entry into the network. Well-crafted IP spoofing can overcome this security. Dynamic firewalls are more intelligent and check the access against several variables in its programmed decision tree and depending on their sophistication can be tough to overcome.[188] An understanding of these systems enables the advanced cyberterrorist to avoid or counter them.

In a similar vein, knowledge of common cryptographic applications and protocols is essential to knowing how to work around them. Weak cryptographic protocols allow text to be easily decrypted. Some protocols are particularly complicated, introducing risks of improper implementation. For example it is possible to defeat cryptography by compromising the integrity of the key distribution process with a *man-in-the-middle attack.*[189]

To put all of these technical requirements (other than programming) in perspective, the burden is roughly equivalent to becoming a Microsoft Certified Systems Engineer, Plus Internet (MCSE +I). As it was intended, this certification requires at least six months of dedicated study.[190]

The organization's improved technical knowledge increases their ability to develop detailed target intelligence. Rather than searching for a target that is vulnerable to the available tool, the terrorist is now selecting the correct tool for the chosen target. If needed, the attacker will use the knowledge gained from the target intelligence to combine or modify existing tools to access the system. To satisfy the information requirements, these groups will conduct a thorough pre-attack reconnaissance.

An organization at this skill level can search through multiple layers of separation and/or indirection in order to locate the desired target. This includes at least some capability to work through firewalls.

In order to test and rehearse the cyberattack, the organization must be able to model the target system. This capability is based on both the computer science knowledge discussed above and the analytical capacity to identify the

---

[188] Brenton, pp.145-164

[189] In this attack, an intruder inserts himself between two communicating parties and impersonates each of them. He provides a false key to each party allowing him to view or manipulate messages. When properly executed, the attack is transparent to the victims, as they appear to be receiving valid messages from one another.

[190] See for example the training program offered by the University of Phoenix. Although there are a number of other organizations that advertise a much shorter study period, they help people "cram" for he examinations without truly mastering the material.

salient features of a given system. The information about the target must include more than just the computer types. The attackers must be sufficiently familiar with any devices connected with the target system to include their effects in the analysis.

A group at this level knows what to look for and how to get it. What they may be unable to do is correctly infer missing or incomplete target information. An absence of complete information will characterize most attacks. This analytical weakness will therefore have an impact on the organization's planning and execution capabilities.

This group has a definite vision of success (though they may not be able to clearly articulate it). Advanced-structured cyberterror activities may exhibit a high degree of sophistication. An advanced-structured attack may consist of many intricate parts. Any group acting at this level will have detailed knowledge about the first order effects of the planned cyberterror activity. They would also have considered and addressed second and third order effects.

One of the key differences between advanced-structured activities and the complex-coordinated activities discussed below is that advanced-structured activities are generally executed sequentially. Events that occur concurrently do so in barrage fashion without much synchronization.

The greatest single area of improvement from the simple-unstructured to the advanced-structured capability levels is in the area of technical expertise. The greatest single limitation to further capability is in command and control. Because of this limitation, all of the technical expertise for a group of this caliber is still likely to reside in a single individual.

3. Complex-Coordinated

The capability for coordinated attacks capable of causing mass-disruption. Ability to analyze vulnerabilities, penetrate complex defenses (including cryptography) and create attack tools. Strong ability to conduct target analysis and high confidence in results. Strong command and control structure capable of employing multiple, simultaneous attacks from different locations. Strong organizational learning capacity – can keep up with latest technology, train personnel, diffuse knowledge throughout the organization, make necessary doctrinal and organizational changes to enhance capabilities.

The group that wishes to strike at large-scale command and control, industrial or infrastructure networks with surety must develop a complex-coordinated capability. These networks are heterogeneous. They consist of varied

hardware and software components. Many of these components are specialized. Knowledge of workstations and web servers will not suffice.

A group with a complex-coordinated attack capability would be an elite organization. The existence of this level of expertise in the underground community is widely rumored but unproven. Estimates vary from source to source, but personnel at this skill level make up an extraordinarily small percentage of the hacker population.

> The Center for Infrastructural Warfare Studies estimated in December 1997 that there were then fewer than 1000 professional hackers worldwide at the time. They defined 'professional hacker' as someone who "is capable of building and creating original cracking methods. He has superior programming skills in a number of machine languages and has original knowledge of telecommunication networks."[191]
>
> Can hackers working from personal computers at home really pose a serious threat to national and commercial security? L0pht thinks it's possible. They've encountered perhaps twelve genius-level hackers in the online world and say six of them should be feared. [192]

In theory, an attacker at this skill level could strike without warning and leave no clues as to his identity. "Pure" cyberterrorism[193] finally becomes possible at this level. Because it is so difficult to achieve, a complex-coordinated attack capability is arguably a group, vice individual, capability.[194] Although there are required technical skill improvements, the primary advancement at this level is in organizational skills. Some sources believe that a charismatic, visionary leader could assemble a group of individuals with advanced-level skills and create a complex-coordinated capability.[195]

---

[191] CIWARS Intelligence Report, Vol. 1, Issue 16, 14 Dec 1997 as quoted in Dorothy Denning, *Information Warfare and Security* (Berkeley, CA: Addison-Wesley, 1999), p. 51. See also John Borland, "Analyzing the Threat of Cyberterrorism," at Infowar.com http://www.infowar.com

[192] Tom Bearden, "Hacking Around" transcript of *The NewsHour with Jim Lehrer,* 8 May 1998. http://www.pbs.org/newshour

[193] Pure cyberterrorism uses only information technology to achieve its aims. This includes everything from information gathering to execution. Pure cyberterrorism is interesting because its success is independent of any target specific factors. It therefore scales infinitely.

[194] For a mythical example see Frederick Cohen, "Managing Network Security – Anatomy of a Successful Sophisticated Attack." *Network Security Management*, Jan. 1999. Available at http://all.net/journal/netsec/9901.html

[195] See DCI 1997 and Douglas Hayward, "Hacker's Dark Side Gets Even Darker" *TechWire.* 19 June 1997. http://www.techwire.com/

A sample cyberterror act in this realm would be sustained, total interruption of some component of the national critical infrastructure across a substantial customer base (i.e. a state or a major metropolis).

A complex-coordinated capability requires superior programming skill. The programmer at this level is capable of writing device drivers.[196] The group has fully mastered at least one high-level language and can write passable programs in any common language. They have also mastered the assembly language for at least one target platform.

Likely targets at this level will have redundancies and back-ups. These protective measures force attackers at this level to master multiple operating systems. The attackers must also be at least comfortable with those systems they have not mastered. This is a substantial requirement. There are at least 42 variants of the UNIX operating system alone. In many systems of interest there are differing, proprietary hardware variations.

Complete interruption of a heterogeneous network demands that attackers develop similar diversity in their tools. They will need to create specialized programs to defeat each of the critical components.

In order to attack the trusted systems in use by command and control systems and other high value targets the organization at this level requires knowledge of advanced security measures. Targeting industrial facilities implies an understanding of industrial computer systems. This includes both Supervisory Controls and Data Acquisition (SCADA) systems as well as Distributed Control Systems (DCS). This is, once again, a challenging technological expertise proposition since there is a wide array of potential protocols and application software to master.[197]

At the previous two levels it was possible to execute an entire attack locally. That is not possible at the complex-coordinated level. This situation demands a deeper knowledge of telecommunications in order to coordinate widely distributed attack elements attackers. An attacker should be able to transmit coordination messages via out-of-band means so as not to be reliant upon the targeted network for communications.

---

[196] Device drivers are the software interface between an operating system and the system (mostly hardware) components. Writing one requires intimate knowledge both of the component and the operating system.

[197] Examples of protocols in use include Modbus, Fieldbus, LonWorks, BACnet and arcnet.

• Expert level programming skill.	• Mastery of multiple operating systems.
• Detailed knowledge of industrial computer systems.	• Detailed knowledge of telecommunications.

Table 5-2: Complex-coordinated Capability IT Expertise Requirements

We have surveyed the available literature and conducted our own scenario development in an attempt to produce the worst-case scenarios of cyberterrorism. We concluded that they tend to revolve around either financial or infrastructure networks. In either case, the terrorist organization must be knowledgeable on two subjects, the computer systems and the controlled process.

In the case of infrastructure networks, the controlled process is some physical activity. Example processes include power generation, air traffic control and the manufacture of potentially harmful materials. The level of target specific information required to attack these targets is that of an insider.[198]

As the magnitude of the target increases, the number of essential elements of information (EEIs) will increase. The intelligence burden for targets of this magnitude will require long term, detailed target reconnaissance using multiple collection methods. Processing the collected information requires a multi-source intelligence fusion capability.[199]

The resident technical experience at this level allows for thorough target intelligence analysis. A near compete understanding of the technical complexity of the network allows for accurate nodal analysis. The greatest limitation to target intelligence at this level is gathering the appropriate information to analyze.[200] Even in the absence of complete information, a complex-coordinated target intelligence capability can infer from traffic analysis some of the system parameters.

Conducting a nodal analysis on a complex network is a substantial undertaking. Studies on network reliability and survivability have examined the

[198] Capt. Barry Ezell USA, "The Risks of Cyber Attack Against Supervisory Controls And Data Automation For Water Supply" (Masters Thesis, University of Virginia, 1998).

[199] These are additional reasons to believe that groups, rather than individuals, must conduct the attacks at this capability level.

[200] An excellent inhibitor to effective target intelligence is for organizations to recognize their critical network and identify the essential elements of information (EEIs) needed to attack their system and then protect these EEIs.

problem of determining the minimum number of links that must be removed for any given pair of hosts to be completely disconnected. This is the analysis that an attacker must perform to ensure success of his attack. For complex networks this analysis can require effort proportional to the square of the number of nodes in the network.[201]

> The Threat and Vulnerabilities Panel concluded that if, with all the knowledge we have about our own systems, we are unable to determine the degree to which effects would multiply and cascade; an adversary would have a far more difficult task of collecting and assessing detailed intelligence of literally hundreds, if not thousands, of networked systems in order to plan and successfully execute an attack of the magnitude which we would consider to be "strategic." The very complexity and heterogeneity of today's systems provide a measure of protection against catastrophic failure, by not being susceptible to the same precise attacks.[202]

Before a group at this level even begins planning, they can be expected to conduct a thorough and unbiased risk analysis. Only if they determine that the prospects for success are good will they proceed. These groups will have very specific criteria for success. The success criteria will include the second- and third-order effects that the attack should produce.

Attacks at this capability level demand the synchronization of widely distributed elements – potentially to within fractions of a second. The attack must be wargamed and rehearsed. Detailed alternate and contingency plans must be developed. These additional plans must also be rehearsed. The attack itself should be conceptualized as a campaign with a series of simultaneous attacks being orchestrated concurrently in time - in a word, swarming. If the target is composed of heterogeneous nodes, the attack will require a separate tool designed for each distinct sub-component. Multiple actors will almost certainly be necessary to handle the volume of activity.

The technical requirements of the complex-coordinated capability level represent at least a doubling of the demands at the advanced-structured level. The command and control requirements present an even greater obstacle. The planning and coordination skills at this level are equivalent to those associated with field-grade officers in the military. Such an officer results from at least six years of practical experience.

---

[201] Douglas R. Shier, *Network Reliability and Algebraic Structures* (New York: Oxford University Press, 1991), p. 18.

[202] Defense Science Board, *Report on Information Warfare Defense* (Washington, D.C.: GPO, 1996), pp. 2-14.

At the complex-coordinated attack level, the demands of the cyberterror effort may impel a displacement of traditional terrorist methods. Leading such an attack demands significant attention. At the organization's strategic level, the terrorist leader's focus is divided between traditional and cyberterror activities. Presented with the competing demands on leadership's time, the strategic decision-maker may focus on the bigger return, in this case most likely the complex-coordinated cyberattack against an information infrastructure.

D. Summary

A cyberterror capability requires a mix of skills. Those component skills do not have to be present in equal measure. An overall capability level is the average of the three component skills. However, the three components are sufficiently intertwined that they grow in parallel.

The barriers to entry at the simple-unstructured capability level are minimal. These barriers become increasingly formidable at each subsequent capability level. It is therefore likely that most groups will opt to remain at the simple-unstructured level. This is further supported by the fact that a great number of cyberterror support activities reside at the simple-unstructured level. Groups that decide to pursue higher levels of capability face potentially large time delays. As we shall discuss in the next chapter, this may imply a need for external support to achieve their aims.

VI. The Path - Developing a Cyberterror Capability

A. Purpose

Having discussed the opportunities, incentives, and required capabilities for pursuing cyberterrorism in previous chapters, this chapter explores how an organization actually develops the intended capability. This is the implementation phase, a necessary second phase of strategy development.[203] During implementation, an organization faces a number of considerations. Generally, it must take into account the actions needed to incorporate major new proposals and articulate a detailed plan of ushering in activities in support of these proposals.[204] The criteria these activities must abide by include that they be technically feasible, politically acceptable to key people within the organization, and be in accordance with pre-existing norms and values of the organization.[205] In chapter four we concluded that cyberterrorism is both politically acceptable and consistent with the norms and values of a minority segment of traditional terrorist organizations.

This chapter builds upon the insights of Chapter Five, regarding cyberterror technical requirements, by introducing implementation options. Technical barriers are an important issue because they influence the organization's decision to develop a cyberterror capability internally, or acquire it externally. Other factors that influence development options to a lesser extent include the organization's context, whether the desired capability is pursued singularly or in tandem with other traditional methods, and sponsorship. The result of this analysis yields a general understanding of the challenges in actually developing a cyberterror capability, as well as insights into how it may be developed.

---

[203] Peter McKiernan, "Strategy Past: Strategy Futures," *Long Range Planning, International Journal of Strategic Management and Corporate Planning* 30.5 (1997): pp.790-798.

[204] John M. Bryson, "A Strategic Planning Process for Public and Non-profit Organizations," *Long Range Planning, International Journal of Strategic Management and Corporate Planning* 21.107 (1998): pp. 73-81.

[205] Bryson, p. 77.

B. Implementation Options

> The key strategic issue in insourcing versus outsourcing is whether a company can achieve a maintainable competitive edge by performing an activity internally – usually cheaper, better, in a more timely fashion, or with some unique capability – on a continuing basis.[206]

A key early choice in acquiring a cyberterror capability is whether to outsource the desired capability, or to develop it internally. This section analyzes the barriers to entry and associated benefits and risks of pursuing either development option from the perspective of an organization interested in cyberterrorism.

1. Barriers to Entry

In the previous chapter, we indicated that an organization wishing to possess the capability to conduct simple-unstructured cyberterror activity faces virtually no technical barriers. The required technical skills are minimal, as are the resource costs. For a simple-unstructured cyberterror capability, no internal organizational learning function needs to be created.

If a group wishes to rise to an advanced-structured cyberterror capability, the technical barriers increase sharply. The required skills described in chapter five are recounted in Table 5-1. It is possible that a group could have one or more members, who already possess a portion of these skills. In this case, the choice to develop internally is clear.

Advanced programming skills.	Mastery of at least one operating system.
Understanding of the mechanics of common security measures.	Detailed understanding of network architectures.
Detailed understanding of the TCP/IP protocol suite.	Familiarity with telecommunications systems.

Table 6-1: Advanced-structured Capability IT Expertise Requirements

If a group does not have pre-existing capabilities a remedial solution to cultivate a more robust program may be to select one or more members from

[206] Henry Mintzberg and James B. Quinn, *The Strategy Process*, 3rd ed. (New Jersey: Prentice Hall, 1996), p. 69.

within the organization to receive training. These members should have a demonstrated aptitude for mathematics and science. If no such members exist, the group cannot realistically pursue this capability internally.

In the previous chapter we introduced several rough metrics for determining the time required to develop a given level of cyberterror capability. The time estimates are summarized in table 6-2. These estimates are calculated for a group starting out with no IT background. The figures represent the total time required to reach the selected capability level. Thus, a group that has developed an experience base through administrative use of IT will have a lead over a group that has not developed a similar base.

By the table 6-2 figures a terrorist group can expect to have an advanced-structured cyberterror capability in a year at best. That accounts only for the academic technical requirements. The one year figure does not account for the practical experience so essential to advanced-structured cyberterror. The need for experience drives our analysis that 2-4 years is more likely. Recall that the CERT®/CC assessment provides a high-end estimate of four years (the undergraduate degree).

We assessed the technical demands of the complex-coordinated cyberterror capability level as double those of the advanced-structured level. Using that assessment results in a minimum figure of two years (one year after achieving advanced-structured capability). At the complex-coordinated level, those technical requirements are likely not the determining factor. Using the field-grade officer analogy of chapter five for command and control provides a likely development time of six years.[207]

A combination of human factors contributes to the barriers in developing a complex-coordinated capability. Individuals must combine training and experience with innate talents. Talents that are genetically granted, not produced through training. However, simply accumulating these individual skills is also not enough. Additionally, terrorist groups wishing to cultivate a complex-coordinated capability must inculcate other individual and group learning characteristics of more highly creative organizations.

[207] Several domain experts have also indicated that 4-6 years is appropriate for developing the required expertise in controlled processes.

> Every knowledge worker in the modern organization is an "executive," if by virtue of his possession of knowledge, he is responsible for a contribution that materially affects the capacity of the organization to perform and to obtain results.[208]

At a complex-coordinated level a terrorist group's ability to assimilate and understand new technology will also influence the organization's capability; i.e. to demonstrate organizational learning. This barrier is the critical obstacle for organizations wanting to attain a complex-coordinated capability. Substantial organizational focus is required to maintain pace with rapidly changing technology. Internal to the organization, cyberterror issues will dominate fiscal commitments. Although hardware purchasing requirements do not increase drastically from the advanced-structured level, the manpower requirements for intelligence collection and analysis will likely create a drain.

In review, the desire to pursue a cyberterror capability must account for substantial barriers to entry at the advanced-structured and complex-coordinated levels. The main obstacle enroute to developing these capabilities falls generally within two categories summarized below.

Cyberterror Level	Skills	Time
Simple-unstructured	Gain Familiarity	0-6 Months
Advanced-structured	Mastery of OS Programming	Min: 1 Year Likely: 2-4 Years
Complex-coordinated	Improve and Combine Advanced-structured Skills with innate talents Organizational Learning	Min: 2 Years Likely: 6-10 Years

Table 6-2: Summary of Barriers to Entry

[208] Peter Drucker, *The Effective Executive* (New York: Harper & Row, 1966), p. 5 as quoted in Ray Grenier and George Metes, *Going Virtual: Moving Your Organization into the 21st Century* (New Jersey: Prentice Hall, 1995), p. 87.

2. Develop Internally

a) Benefits of Internal Development

Organizations benefit from internal development in several ways. If done internally, the organization gains greater independence. Real problems can occur when external sources do not share the same priorities as the organization seeking their product or service.[209]

Internal development also enhances security, a critical interest of all terrorist organizations. Not having to rely on external interactions reduces the risk of exposure during electronic and personal interactions with outside parties. Internal development also eliminates unpredictable security arrangements normally associated with most outsourcing solutions.

Finally, internal development may facilitate interactions among skilled people in different functional areas. This form of interaction may augment the groups' knowledge base while increasing organizational creativity.

b) Risks of Internal Development

Perhaps the single greatest risk in developing cyberterror capabilities internally may result from failing to develop an effective capability. In other words, the organization is unable to cultivate an advanced-structured or complex-coordinated capability, or prematurely exposes it. Failure, in this case, would lead to ineffectiveness as an organization, irrelevance and possibly extinction.

Additionally, internal transaction costs of pursuing advanced-structured and complex-coordinated capabilities may be extremely high. If a terrorist organization is to produce these capabilities internally on a long-term basis, it must be prepared to finance research and development, personnel development, and infrastructure investments. If incorrectly assessed, the organization may lose precious amounts of limited financial resources.

At the individual level, terrorist groups also risk loosing key personnel before necessary training can be provided. This "brain drain" may affect terrorist organizations in the same way it has other IT companies. Unless the incentives of membership in a terrorist organization offset the monetary incentives associated with pursuing legitimate IT professions terrorist groups

---

[209] Mintzberg and Quinn, p. 72.

may never adequately recruit potentially gifted members.[210] The following list of IT salaries is evidence of the monetary incentives for pursuing legitimate professions that terrorist organizations must contend with.

Job Title	1998 Average Salary	1998 Average Bonus
CIO/VP of Information Systems	$99,100	$17,000
Director of Information Systems	$73,000	$8,700
Director of networks	$66,800	$5,600
Network Administrator	$46,300	$2,400
Senior Systems Analyst	$56,700	$2,700
Systems Programmer	$48,100	$2,400
Database Analyst	$54,300	$3,600

Table 6-3: Average IT Salary Data[211]

3. Acquire Externally

An alternative to developing these capabilities internally is outsourcing. We identify two general forms of outsourcing. The first is through open-source markets. The second form of outsourcing is to cultivate the necessary capabilities with a sponsor.

---

[210] Even in the absence of a salary, the terrorist organization will be competing against the cyber 'terrorists' expectations for a standard of living. Individuals with advanced or complex-coordinated technical expertise must forego market valuation of their skills to provide the necessary commitment to the terrorist organization.

[211] Leslie Goff, "Enough is Enough, Computerworld's 12th Annual Salary Survey," *Computerworld*, 7 Sept. 1998, pp. 56-61. Available online at: http://www.computerworld.com/home/features.nsf/All/980907mgt2

a) Open Sources

In a general sense, outsourcing provides necessary skills, services or products that the organization is either unable to develop, or based upon other criteria, may be more cost-effectively acquired elsewhere. Typically, the tasks acquired externally are beyond the core interests of the organization. "Most companies will benefit by extending outsourcing first in less critical areas."[212] However, in the case of organizations considering development of a cyberterror capability, most must consider outsourcing critical skills and products because they simply are not available inside the organization.[213] Beyond deciding what to outsource, an organization must also consider the following criteria: security, availability, cost, timing and the reliability of the outsourcing endeavor.

(1) Benefits of Outsourcing

The benefits of outsourcing a cyberterror capability include timeliness, cost-efficiency and security. As discussed previously, many of the skills necessary to conduct complex-coordinated attacks can only be found outside conventional terrorist organizations. Over time, assuming the organization intends to develop an internal capability, this will change. Until then, the fastest method of developing simple-unstructured, advanced-structured or complex-coordinated capabilities is via outsourcing. Therefore, timeliness is an important issue in the consideration of outsourcing.

Until recently, the main attraction to outsourcing was cost efficiencies.

> Savings of between 30 and 70 percent, can be obtained -- estimates vary -- largely because of the reduced staff costs.[214]

Cost efficiencies of this kind may significantly benefit those organizations interested in developing a cyberterror capability. The banking industry provides an instructive example of successful outsourcing. Banks share some of the security concerns held by terrorist groups. Many banks have discovered that they cannot afford to keep up with the rapid pace of technological change on their own. Those banks have entered into contracts with third-party

---

[212] Mintzberg and Quinn, p. 69.

[213] Of the groups presented in Jane's *World Insurgency and Terrorism* only six were shown having any cyberterror capability. All were at the simple-unstructured level according to our taxonomy.

[214] Jim Hayes, "Offshore IT providers ready for business after year 2000," *IT Week Online*, 3 May 1999. http://www.zdnet.co.uk/itweek/brief/1999/17/offshore/01.html.

processing companies that have developed as a result of consolidation and the pursuit of operating efficiencies within the financial services industry.

Typical services offered by third-party processors include the following:

- Data center management
- Network management
- Application development, management and maintenance
- Check and statement processing
- Mutual fund account processing
- Electronic funds transfer
- Core technology implementation and support.[215]

These outsourcing efforts have been so successful that some banks have even outsourced whole departments. In fact, over 10 percent of checks and sixty-eight percent of credit card accounts are now processed by these third party technology providers.[216]

Finally, outsourcing may augment security arrangements within terrorist organizations. Security equates to essentially two areas concerning terrorist organizations. Terrorist groups, of necessity, must remain a secret to both state and international counter-terror operations. Security is also achieved by maintaining anonymity within the group. In other words, the less constituents within the organization know and understand about the group overall, the better the security. In the same way, many military secrets are kept secret by compartmentalizing. Outsourcing is a creative means of compartmentalizing within the terrorist organization, assuming it is done properly. Many of today's network tunneling protocols support this arrangement. One of these protocols is the Point-to-Point Tunneling Protocol (PPTP).[217] PPTP allows organizations to use the Internet as a secure private network. Merrill-Lynch and TRM Inc.,

---

[215] Joanna Bers, "Outsourcing It All," *Bank Systems*, March 1996 as quoted in The President's National Security Telecommunications Advisory Committee (NSTAC), *Financial Services Risk Assessment Report* (1997), p. 20. All of the NSTAC reports are available online at http://www.ncs.gov/nstac/NSTACreports.html

[216] NSTAC, *Financial Services*. The top five such service providers in the United States are ALLTEL Information Services Inc, BISYS, Electronic Data Systems Corp., Fiserv Inc., and M&I Data Services.

[217] American Research Group, *Windows NT 4.0 Security* (ARG, 1998), p. 10-2.

among others, have adopted this technique to protect some of their electronic interactions.[218]

(2) Risks of Outsourcing

Alternatively, the risks associated with acquiring a capability externally include reliability and availability. Unlike most outsourcing issues, in the case of cyberterror, the terrorist organization is likely to seek all, or a majority of their cyber-capability, by a third party. Can the organization depend on an outside source to provide these skills?

> The most successful outsourcers find it absolutely essential to have both close personal contact and rapport at the floor level and political clout and understanding with the supplier's top management.[219]

For obvious security reasons terrorist organizations seeking to outsource with legitimate vendors will be unable to maintain close contact and rapport.

There are numerous security concerns when groups are forced to exercise outsourcing solutions. Because cyberterror at the advanced-structured and complex-coordinated levels is so difficult to understand it will be very difficult to conduct quality control assessments on an outside agent. The risk that their external source is either compromised or incompetent may be too great for a terrorist organization. Likewise, there is a certain amount of risk associated with the collection of hacker tools. It is possible that the terrorist group may get "hacked" while attempting to find tools. There have been incidents of hacker tools that contained Trojan horses directed against the tool user.[220] The risk of being victimized on the Internet is certainly no greater than the risk of outsourcing to an untrustworthy or incompetent agent.

The final issue with regard to outsourcing is availability. IT skills and equipment are disseminating globally. IT skills are not confined to the Western world.[221] Those skills that cannot be accessed in person, are increasingly accessible via communication media.

---

[218] Microsoft press release retrieved from http://www.microsoft.com/ntserver/commserve/solutions/default.asp.

[219] Mintzberg and Quinn, p. 72.

[220] Two examples include the programs Wartools and WinSATAN.

[221] Hayes, http://www.zdnet.co.uk/itweek/brief/1999/17/offshore/01.html.

> Advances in global communications mean that projects can be coordinated in real time, with code and other collateral being transmitted backwards and forwards with ease.[222]

However, can this form of remote access be trusted? The same vulnerabilities associated with the Western infrastructure dependencies are likely to affect groups that rely on remote access.

b) Sponsorship

An alternative to externally acquiring a cyber capability from an open source vendor is through sponsorship.

> Sponsorship refers to the assistance a terrorist group receives from states, non-states or other terrorist organizations. Assistance, in this case, may take the form of personnel, basing, training or resourcing. It may be provided for a specific target, series of targets, a duration of time, or toward the development of a general capability.

The U.S. State Department recognizes seven countries offering sponsorship to terrorist organizations. These are Sudan, Syria, Iran, Iraq, Libya, North Korea, and Cuba. Additionally, Burma, Yemen, Egypt, Uganda, Eritrea and Ethiopa are identified as potential supporters. Of the known sponsors, Iran poses the most serious threat.

> Iran continued to provide support to a variety of terrorist groups, including the Lebanese Hizballah, HAMAS, and the Palestinian Jihad, which oppose the Middle East peace process through violence. Iran supports these groups with varying amounts of training, money, and/or weapons.[223]

What may be more disturbing about Iran, however, is that it is likely developing a comprehensive Information Warfare capability as well.

State sponsors with IW programs may benefit by sharing these capabilities with terrorist groups. By making these capabilities available to terrorist groups sponsors are provided a means of testing specific capabilities while also

---

[222] Hayes, http://www.zdnet.co.uk/itweek/brief/1999/17/offshore/01.html.

[223] Department of State, *Patterns of Global Terrorism: 1998*, Overview of State-sponsored Terrorism, p. 4 of 7, http://www.state.gov/www/global/terrorism/1998Report/sponsor.html

maintaining deniability. Terrorist groups benefit in this arrangement by potentially gaining access to advanced-structured and complex-coordinated cyberterror capabilities.

4. Summary of Implementation Options

> The key strategic issue in insourcing versus outsourcing is whether a company can achieve a maintainable competitive edge by performing an activity internally – usually cheaper, better, in a more timely fashion, or with some unique capability – on a continuing basis.[224]

Assuming a terrorist group has sufficient resources, time, and at least fundamental technical expertise, one would expect a cyberterror capability to be developed internally. However, the technical skills necessary to accomplish advanced-structured and complex-coordinated capabilities are formidable, and even if they were attainable, the time it would take to cultivate these skills may be at odds with the group's interests. Therefore, terrorist organizations may choose to acquire all or part of these capabilities externally. The options, in this case, are to acquire these functions from open source providers or to seek support from terrorist sponsors with IW programs.

C. Organizational Contexts

In the remaining sections of this chapter, we test the general implementation options presented above against four general organizational contexts. This analysis highlights whether certain organizational settings are more, or less, inclined to develop advanced-structured and complex-coordinated capabilities. The contexts presented are *newly formed* organizations, *splinter* groups, *stable* organizations and organizations in *decline*.

a) *Newly Formed* Organizations

> *Newly formed* organizations operate in the entrepreneurial stage of organizational life cycle development. Organizations in the entrepreneurial stage are in their infancy. They are informally structured, highly creative and share ambiguous goals. Osama Bin Laden's "Al Qaeda" is the closest example of an organization in this category.

Newly formed organizations may be favorably inclined toward cyberterror under the following conditions:

---

[224] Mintzberg and Quinn, p. 69.

- When relying on a "core competency" to break into the "competitive market" may seem attractive.

- When they are flexible enough to have the option of fully developing a cyberterror capability, or to outsource specific needs.

- When they do not need to rely on sponsorship for resourcing or development issues.

Newly formed organizations may gain a competitive advantage by concentrating on a core competency. First, the organization maximizes returns on internal resources by concentrating on what it does best. Second, fully developed core competencies provide flexible barriers to change in the organizations competitive environment by reducing risks, shortening development timelines and lowering investments. Third, perhaps most importantly, is the potential to fully utilize external suppliers, innovations and professional capabilities that may be prohibitively expensive or impossible to duplicate internally.[225]

Newly formed organizations may have the luxury of insourcing; i.e. not relying on a sponsor or other outsourcing option. Simple-unstructured capabilities can be pursued internally with relative ease. Given the skills and resources needed to develop a simple capability, newly formed organizations can readily access the resources and personnel necessary. The newly formed organization capable of overcoming the significant technical barriers to develop an advanced-structured or complex-coordinated capability internally will benefit from greater security and independence. By developing the capability internally, the organization is neither forced to surrender its independence to an external sponsor, nor subject to the risks and unpredictable security of most outsourcing options.

To implement advanced-structured or complex-coordinated capabilities however, may require a significantly greater expenditure of time and resources than a newly formed organization may otherwise have available. The decision to implement these capabilities internally must be met with an acceptance that it will take significantly longer, cost significantly more, and ultimately, may jeopardize the group's transition to later stages of development. To mitigate these factors, the organization may conceive an implementation strategy that involves outsourcing specific functions.

Newly formed organizations may outsource for the following reasons:

[225] Mintzberg and Quinn, p. 64.

- The organization actively develops a capability internally but is far from able to conduct any sort of credible attack.

- The organization chooses temporarily to outsource advanced-structured and complex-coordinated capabilities from a sponsor, other terrorist organization, hacker group or TCO.

- Outsourcing is used because it allows the organization to claim a capability long before it is able to develop one internally.

Outsourcing may be done in support of a single or a finite number of operations. The benefit of outsourcing is to access quickly the advanced-structured and complex-coordinated capabilities that would take much longer to develop internally. However, this benefit must be weighed against the security risks of acquiring the capability externally addressed in previous sections.

To summarize, newly formed organizations are suitably inclined to pursue cyberterror through internal development or external acquisition. They will likely attempt to develop core competencies internally, while acquiring less essential cyber activities from outside vendors. It is possible, however unlikely, that newly formed groups would seek to develop advanced-structured or complex-coordinated capabilities with a sponsor; because this would unnecessarily require them to surrender their independence and some level of anonymity.

b) *Splinter* Groups

Splinter groups feature some of the characteristics of an organization in the entrepreneurial stage of development, as well as characteristics of a stable organization. The Al-Gama'a al-Islamiyya (GAI), an Egyptian Islamist group responsible for the murders of 58 tourists and four Egyptians in November 1997, is an example of a recently "splintered" terrorist group.

Splinter groups are inclined to implement a cyberterror strategy through external acquisition, for the following reasons.

- They must be willing to accept disruption as a suitable substitute for destruction in pursuit of a cyberterror strategy.

- They must rely on external acquisitions or sponsorship to provide necessary advanced-structured or complex-coordinated capabilities.

- They are inherently predisposed to a given set of cultural and organizational constraints that other newly formed or stable organizations are not, due to the nature of their formation.

- Most often, they leave their former organizations in support of a specific agenda, typically violent in nature.

Splinter groups are unlikely to engage in cyberterror. Simple-unstructured cyberterror (hacking, defacing web sites, etc.) does not provide a group psychological rewards comparable to the violent acts traditionally seen from splinter groups. Advanced-structured and complex-coordinated cyberterror may produce the level of destruction or disruption to meet the organizational/psychological desires of the splinter group. However, given the technical barriers associated with pursuing advanced-structured and complex-coordinated capabilities, it is unlikely that splinter organizations will be able to perpetrate disruptive attacks without outside assistance.

This means that if they undertake to develop a cyberterror capability, splinter groups will likely pursue an outsourcing strategy because it provides immediate access to advanced-structured, and possibly complex-coordinated, capabilities. Splinter organizations are more likely to acquire these capabilities from a sponsor than through other legitimate forms. In the case of splinter organizations, likely sponsors include other terrorist organizations, non-state actors, or states such as Iran.

Assuming the technical barriers can be overcome, splinter organizations must also overcome their ingrained cultural and political obstacles to pursuing any form of cyberterror. The set of norms, experiences and accepted relationships that exist within splinter groups are often disincentives for adopting cyberterror. Typically, these groups share a common belief that increased violence and action are necessary means of coercion. This belief is often the driving force behind their group's movement away from organizations perceived to be less aggressive.

To summarize, this organizational context facilitates the pursuit of cyberterror, but only if disruption is accepted as suitable feedback, and the advanced-structured and complex-coordinated capabilities necessary to accomplish mass disruption, can be acquired externally.

c) *Stable* Organizations

> Stable organizations have a history of development that includes some or all of the following organization life cycle stages: collectivity, formalization and control or elaboration. Organizations in the collectivity stage characteristically have informal structures, clear goals, and high personal commitment. Organizations in the formalization stage characteristically have stabile structures, formalized activities, and conservative decision-making. Organizations in the elaboration stage perform diverse activities, search for growth opportunities, practice decentralized decision-making, and are structurally more complex. Hamas, Provisional Irish Republican Army (PIRA), Groupe Islamique Arme (GIA), Hezbollah, Ejercito de Liberacion Nacional (ELN) are all examples of stable organizations.

Stable organizations are inclined to pursue a cyberterror capability for the following reasons.

- They enjoy stable funding, practice thorough training and have a regular supply of personnel (whether indigenous or provided by a sponsor).
- They can more easily add cyberterror to other existing "specialties."
- They are procedurally efficient.
- They are more protected against adversity in the environment although, they may be slow to respond to change.

Stable organizations enjoy the benefits of strong support. This support extends to funding, basing, training, equipment and personnel. Whether these areas are indigenous to the organization or provided by an outside sponsor depends upon the organization in question.[226] However, the fact that these are available broadens the scope of what the organization can pursue. Having a strong support base provides the would-be cyberterrorist with the flexibility to pursue traditional forms, protection against emerging challenges and a relative sense of independence.

Stable organizations may be motivated to pursue cyberterrorism in conjunction with other traditional forms of terrorism. Appending cyberterror to traditional terrorism is a form of "related diversification." Related diversification, if done properly, benefits the organization by providing operational and

[226] This report is not designed to address each organization. Instead we are trying to identify why these support relationships exist and how the organization benefits.

administrative synergies, and economies of scale with other traditional terrorist functions.[227] A symbiosis with traditional terrorist methods and cyberterror attack can occur. An organization begins to integrate the cyberterror attack capability into the operation of the organization. With this introduction of a new terrorist 'tool' the organization will develop internal processes and control mechanisms to manage the new 'operational' capability. This new complementary operational capability is not likely to diffuse throughout the terrorist organization though. For example, each terrorist operative within the organization would not be trained in cyberterror attack. The capability would reside within a cyber cell whose activity would be coordinated to support a traditional operation.[228] Similar to the way terrorist organizations value skilled bomb-makers and as previously noted in our section on task specialization (chapter four):

> Within a terrorist organization, a distinction is often made between the bombmaker, who never goes near a target and whose skills are carefully preserved, and the other operatives who risk arrest and premature detonations while planting the devices.[229]

The ability to use secure e-mail and construct anonymous web pages are examples of ways the organization may improve command, control and communications within the organization's cells. These abilities may grow and provide the necessary capability to conduct simple-unstructured cyberterror attacks such as "smurfing." However ineffective as coercive instruments, simple-unstructured attacks may also serve as useful advertising and propaganda tools for the traditional terrorist.

---

[227] Brian K. Boyd, Sydney Finkelstein, Harry Barkema and Luis Gomez-Mejia, "Matching Diversification and Compensation Strategies," *New Managerial Mindsets: Organizational Transformation and Strategy Implementation*, ed. Michael A.. Hitt, Joan E. Ricart i Costa and Robert D. Nixon (New York: Wiley, 1998), p. 170 and Mintzberg and Quinn, p. 717.

[228] Drawing from Henry Mintzberg, *Structures in Fives – Designing Effective Organizations* (Englewood Cliffs, NJ: Prentice Hall, 1993), we propose that the new (advanced-structured capable) cyber cell within a previously traditional terrorist organization most likely will reside within the organization's support structure and not within the operating core where a number of levels of management would reside between the cyber capability and the organization's strategic apex (leadership).

[229] Sommerville, p. 217.

> In February 1995 supporters of the Ejercito Zapatista de Liberacion Nacional (EZLN) posted messages on several Internet news groups alleging that the Mexican Army was subjecting villages in Chiapas to random airborne bombardment, killing unarmed civilians in large numbers. However, investigative journalists who visited the area were unable to find any evidence to confirm the reported incidents.[230]

Stable organizations may benefit from the pursuit of cyberterrorism in another way. The redundancies that may be realized with the development of a cyberterror capability will provide organizational "slack."[231] These redundancies protect the organization from sudden changes in their environment. Redundancies are also a cost-effective way of supporting two divergent capabilities, for the price of one.

Stable organizations are likely to benefit from the added efficiencies and unintended consequences that result from embracing IT. The internet, cellular communications and facsimile all combine to enhance distributed, difficult to trace communications traffic among and between terrorist organizations, their members and their sponsors. The devices used to initially support traditional terrorism administratively may some day be used to conduct operations in the form of cyberterror attack.

To summarize, stable organizations are likely to pursue cyberterrorism because it can be easily appended to other existing specialties, they will enjoy enhanced performance organizationally, and it protects them from adversity in their environment.

d) Organizations in *Decline*

> Organizations in their decline realize a significant loss of personnel while suffering decreased demand from their competitive market. These organizations are on the verge of extinction, or at least irrelevance. Abu Nidal, Islamic Brotherhood and the Red Brigades are examples of organizations in this category.

Of all the categories reviewed, organizations in decline are least capable of cultivating a cyberterror capability for the following reasons.

---

[230] Jane's Information Group Limited, *World Insurgency and Terrorism* (UK: DPA Publishing, 1998).

[231] Herbert A. Simon, *Administrative Behavior*, 4th ed. (New York: The Free Press, 1997).

- They tend to rely on existing methods rather than other, more creative approaches.

- They look toward increasing violence to reverse their growing ineffectiveness as an organization.

- They do not have the benefit of time to develop advanced-structured or complex-coordinated capabilities and it is unlikely that external sources would provide these capabilities.

- Although most likely to seek sponsor support to develop a capability, it is unlikely to be in the best interest of a sponsor to invest in a declining group.

Organizations in decline, rather than trying something new, tend to rely on previously used methods. The historical trend among those groups that go into decline has been both to rely increasingly on previously successful attacks as well as to increase their frequency. During decline, the terrorist group is at its most dangerous. The group needs to get back in the game. To do so, publicity and headlines are necessary.[232]

Similarly, organizations in decline tend to rely on increased violence (hyperviolence) in a final effort to regain political coerciveness. As discussed earlier, the most likely results of cyberterror range from moderately disruptive at the simple-unstructured level to massively disruptive, and perhaps moderately destructive, at the advanced-structured and complex-coordinated levels. To date however, neither mass disruption, nor destruction has been achieved in the realm of cyberterror.

Finally, organizations in decline are in a race against the clock. Declining organizations have neither the time to consider nor to implement new strategies that may revive their cause (assuming they could accomplish disruptive or destructive effects). Assuming an organization in decline is interested in pursuing a cyberterror attack, it would be forced to acquire this capability externally.

Unlike newly formed organizations and splinter groups, declining organizations are not likely to benefit by external acquisitions. First, organizations in their decline are unlikely to have the finances needed to acquire the personnel and hardware from an external source needed to pursue advanced-structured and complex-coordinated capabilities. Secondly, the benefits of sponsoring an organization in decline may not offset the

[232] Lockett, p. 49.

inherent risks of being associated with this group. As the incentives for group participation deteriorate, members exit in pursuit of other personal interests.[233] Any sensitive information concerning sponsor relationships or specific cyber-capabilities that the group may have attempted to develop before its dissolution may therefore be subject to public disclosure.

To summarize, organizations in decline are less likely to implement a cyberterror strategy. They are not likely to accept the disruptive effects made possible by cyberterror attacks in exchange for repetitive, and violent, traditional acts. They are also less likely to benefit from external acquisition options because of the inherent risks of associating with an organization dangerously near extinction.

D. Conclusions

By testing the general development options presented earlier in this chapter against each of the four general organizational contexts above we now have a sense of which organizations are more likely to pursue advanced-structured and complex-coordinated cyberterror capabilities. We also have a general understanding of how these groups may develop these capabilities. The following table summarizes these results.

[233] Lockett, p. 50.

	Develop Internally	Develop Externally	
		Acquire	Sponsor
Newly Formed	√	√	
Splinter Group		√	√
Stable	√	√	√
Organizations in Decline			√

Table 6-4: Development Summary

- Newly formed organizations will likely attempt to develop a cyber capability internally while acquiring less essential activities externally. It is possible they will develop advanced-structured or complex-coordinated capabilities with a sponsor.

- Splinter groups will pursue cyberterror if disruption is accepted as suitable feedback, and the advanced-structured and complex-coordinated capabilities necessary to accomplish mass disruption, can be acquired externally.

- Stable organizations are likely to pursue cyberterrorism as an adjunct to other existing specialties.

- Organizations in decline are unlikely to implement a cyberterror strategy unless supported by a sponsor.

VII. Conclusions

Threat analysts warn us of our vulnerabilities yet overlook our strengths.[234]

A. Overview

This report takes a balanced approach to analyzing the threats associated with cyberterrorism. This analysis, based upon organizational long-range planning, reviewed the internal and external factors that influence a terrorist group's strategic decision processes. It consisted of an assessment of the operational environment, taken from the perspective of a terrorist organization. This was undertaken by reviewing the strategic and organizational incentives for pursuing the opportunities identified in the previous analysis. Next, an analysis of what was required to pursue cyberterrorism was done, also from the perspective of a terrorist organization. Finally, a review of the options for developing a capability were presented.

The first step of the process was to determine if there was an opportunity in the environment that traditional terrorist organizations could leverage. We concluded that the future will likely feature a continuing utility for traditional terrorism, as well as facilitate the pursuit of cyberterrorism.

The second step called for an assessment of whether this identified opportunity was consistent with the strategic interests, group ideologies and the other personal and organizational incentives held by traditional terrorist groups. We concluded that a minority of traditional terrorist organizations are likely to pursue cyberterrorism.

The next step was to determine whether it is feasible for an organization with little or no existing cyber-capabilities to seek cyberterror. We first presented a generic assessment of what an organization must do to produce simple-unstructured, advanced-structured and complex-coordinated capabilities. This took into account the individual and organizational technical skills and resources necessary to achieve each level.

This assessment was followed by an analysis of the general implementation options that could be used to develop a desired capability. We concluded that the technical barriers to entry, although insignificant at the simple-unstructured level, are significant for advanced-structured and complex-coordinated levels. Additionally, organizations generally have two implementation options –

[234] Ralph Peters, *Fighting for the Future*, p. 205

outsource or develop a desired capability internally. However, this decision is largely dependent upon the context of the organization (newly formed, splinter group, stable or declining).

For the near-term future, advanced-structured and complex-coordinated cyberterrorism will likely be achieved by only a few terrorist organizations. The most dangerous eventuality will likely come from a newly formed, religious group. However, we see this as a long-term threat. A more likely, near-term threat may be posed by stable, new age terrorist groups. Several less dramatic threats at the simple-unstructured and advanced-structured levels were also identified in this analysis that may merit further consideration.

We can expect cyberterror to be developed in iterative stages. Initially, support activities will precede attacks because the Internet and other communications media are readily available. The Zapatistas and Tamil Tigers provide evidence of simple-unstructured capabilities already existing. Simple-unstructured capabilities – support and attack - will continue to be the order of the day until more advanced-structured and complex-coordinated capabilities have had time to develop (either internally or through sponsor programs). At first, cyberterror is likely to accompany other traditional forms of terrorism. However, as complex-coordinated capabilities are developed, it will likely exist independent from traditional terror. When cyberterrorism reaches this point, it will be in its most dangerous and difficult form to defend against.

Our greatest fear is the development of a capability at the edge of all the areas we've considered. In other words, a group formed specifically to capitalize on the most destabilizing aspects of the future environment using a combination of conventional and unconventional practices in an effort to develop the most creative, organic and well-led organizations yet conceived. We have already encountered hierarchies and tomorrow's virtual teams. Fred Cohen's *Anatomy of a Successful Sophisticated Attack* presents a scenario depicting the creative and destructive potential of these highly organic organizations.[235] What is troubling about Cohen's account is that it is based upon attacks that have already occurred.

An organization that is formed in pursuit of a complex-coordinated capability, but is not limited to using this capability remotely, is more likely, yet equally as dangerous. An organization that:

- *Projects* traditional terrorist operatives over-the-horizon that are skilled in infiltrations, shootings, bombings and barricades;

[235] Cohen, "Anatomy of a Successful Attack," http://al.net/journal/netsec/9901.html.

- *Communicates* using a suite of IT devices capable of reaching back to a clandestine command and control center;

- Is *supported* by nontraditional terrorist personnel capable of developing, using, and remotely orchestrating the most insidious and complex cyberterror attacks imaginable, and;

- Is *coordinated* by a new breed of terrorist leader who demonstrates both competence and creativity.

This form of cyberterror, which relies on gaining physical access, enhanced communications, sophisticated hacking techniques and thorough target intelligence is likely to present the greatest threat to our infrastructure in the mid-term future (i.e., a decade out).

B. Recommendations for Future Research

This report suggests starting points for several other research efforts. The first calls for an application of current intelligence data on known and suspected terrorist organizations and their sponsors to the framework presented here. The database available to the authors of this report was a fraction of what is otherwise available to the DIA, CIA and the DOD. Optimally, one or all of these agencies may elect to cull the necessary data, then analyze it using the framework presented in this study.

This framework is a useful tool for both profiling terrorist groups and establishing a cyberterror database. Using the typologies established in this study, the intelligence community now has a useful starting point for establishing and maintaining group profiles according to simple-unstructured, advanced-structured and complex-coordinated cyberterror capabilities. Similar to existing terrorist databases, this database will consolidate raw intelligence data from distributed sources and categorize this information according to the categories described in this report.

As noted in the introduction, this report focused on terrorist organizations outside the United States. To be both accurate and thorough, it must also be applied to domestic terrorist groups as well. An arrangement should be made to allow the appropriate agency, or interagency group, to apply this framework to domestic groups and then share these results with both federal and state agencies.

Additionally, an effort must be made to apply future data to this framework. In this case the data must be interpolated from one, or several, forms of future forecasts. Examples of these include assumption-based planning and

scenarios. The point here is not to decide which form of future planning model to use, but rather to use the model to develop a general set of data that may also be applied to this framework. In other words, to apply the framework to an environmental context that is 15-20 years in the future. Although unpredictable now, this future context will likely present a new set of assumptions and technical possibilities that today may not even seem feasible. However, to be successful this effort to 'run' future data through the framework must first consider the need for model revision. In other words, the framework developed in this study is only applicable to the data available today. Analysts must be wary of any indicators in the future that may suggest the need to revise the model.

Finally, there are two remaining points that should be considered regarding future research. Because of its simplicity, this framework is generally applicable to a number of intelligence problems. One example is to apply this framework to an analysis of terrorism and WMD use. In this case, the need for revision must again be considered. Second, although not a goal at its inception, this project can be viewed as a catalyst for the development of an intelligence threat assessment and early warning system that can be shared by all counter-terror agencies. In this way, we may begin to grapple with the daunting organizational challenges that bedevil the fight against terror.

Appendix A – Global Connectivity Statistics

Country Name	Teledensity per 100 inhabitants
Afghanistan	0.13
Albania	2.33
Algeria	4.75
Andorra	43.14
Angola	0.54
Antigua & Barbuda	40.81
Argentina	19.13
Armenia	14.95
Australia	50.45
Austria	49.18
Azerbaijan	8.69
Bahrain	24.57
Bangladesh	0.26
Barbados	40.43
Belarus	22.66
Belgium	46.81
Belize	13.69
Benin	0.64
Bhutan	1.04
Bolivia	6.88
Bosnia	8.00
Botswana	5.64
Brazil	10.66
Bulgaria	32.26
Burkina Faso	0.33
Burundi	0.26
Cambodia	0.18
Cameroon	0.54
Canada	60.95
Central African Republic	0.29
Chad	0.11
Chile	17.98
China	5.58
Colombia	14.75
Comoros	0.84
Congo	0.82
Costa Rica	16.86
Croatia	33.53
Cuba	3.36
Cyprus	56.97
Czech Republic	31.84
Congo	0.04

Korea Dem.People's Rep.	4.82
Democratic Republic of Congo	0.04
Denmark	63.33
Djibouti	1.31
Dominica	25.23
Dominican Republic	8.76
Ecuador	7.53
Egypt	5.57
El Salvador	5.61
Equatorial Guinea	0.89
Eritrea	0.57
Estonia	32.10
Ethiopia	0.26
Fiji	9.19
Finland	55.59
France	57.61
French Guiana	29.85
French Polynesia	23.04
Gabon	3.27
Gambia	2.13
Georgia	11.41
Germany	54.98
Ghana	0.58
Greece	51.61
Greenland (Denmark)	41.66
Grenada	26.10
Guadeloupe	39.62
Guam	45.31
Guatemala	4.08
Guatemala	4.08
Guinea	0.26
Guinea Bissau	0.69
Guyana	6.52
Haiti	0.80
Honduras	3.68
Hong Kong	56.54
Hungary	30.42
Iceland	61.69
India	1.86
Indonesia	2.47
Iran	10.73
Iraq	3.19
Ireland	41.14
Israel	44.98
Italy	44.68
Jamaica	14.03

Japan	47.86
Jersey	70.00
Jordan	6.97
Kazakhstan	10.80
Kenya	0.81
Kiribati	3.06
Korea, Republic Of	44.40
Kuwait	22.74
Kyrgyzstan	7.56
Lao PDR	0.51
Latvia	30.16
Lebanon	17.86
Lesotho	0.96
Liberia	0.22
Libya	6.79
Lithuania	28.29
Luxembourg	66.87
Macau	40.48
Madagascar	0.27
Malawi	0.35
Malaysia	19.49
Maldives	6.58
Mali	0.20
Malta	49.76
Martinique	42.78
Mauritania	0.55
Mauritius	19.52
Mayotte	7.55
Mexico	9.60
Micronesia	7.58
Moldova	14.54
Mongolia	3.66
Morocco	5.00
Mozambique	0.36
Myanmar	0.46
Namibia	5.76
Nepal	0.77
Neth. Antilles	36.59
Netherlands	56.43
New Caledonia	24.12
New Zealand	48.57
Nicaragua	2.94
Niger	0.17
Nigeria	0.36
Norway	62.11
Oman	8.35

Pakistan	1.85
Panama	13.44
Papua New Guinea	1.07
Paraguay	4.29
Peru	6.75
Philippines	2.83
Poland	19.43
Portugal	40.25
Puerto Rico	35.07
Qatar	24.94
Reunion	35.13
Romania	13.98
Russia	18.27
Rwanda	0.28
Samoa	5.06
Saudi Arabia	11.72
Senegal	1.32
Seychelles	19.56
Sierra Leone	0.39
Singapore	54.29
Slovakia	25.86
Slovenia	36.40
Somalia	0.15
South Africa	10.72
Spain	40.32
Sri Lanka	1.70
Sudan	0.40
Suriname	14.62
Swaziland	2.81
Sweden	67.93
Switzerland	66.09
Syria	8.78
Taiwan	49.96
Tajikistan	3.77
Tanzania	0.33
TFYR Macedonia	20.38
Thailand	7.96
Togo	0.58
Tonga	7.90
Trinidad & Tobago	19.01
Tunisia	7.02
Turkey	25.04
Turkmenistan	7.80
UAE	35.09
Uganda	0.25
Ukraine	18.56

United Kingdom	54.00
United States	64.37
Uruguay	23.20
Uzbekistan	6.30
Vanuatu	2.57
Venezuela	11.06
Viet Nam	2.07
Yemen	1.34
Yugoslavia	20.58
Zaire	0.50
Zambia	0.91
Zimbabwe	1.72

Appendix B – Bi-Lateral Extradition Treaties

1. Albania
2. Antigua & Barbuda
3. Argentina
4. Australia
5. Austria
6. Bahamas
7. Barbados
8. Belgium
9. Belize
10. Bolivia
11. Bosnia-Herzegovina
12. Brazil
13. Bulgaria
14. Canada
15. Chile
16. Colombia
17. Congo
18. Costa Rica
19. Croatia
20. Cuba
21. Cyprus
22. Czech Republic
23. Denmark
24. Dominica
25. Dominican Republic
26. Ecuador
27. Egypt
28. El Salvador
29. Estonia
30. Fiji
31. Finland
32. France
33. Gambia
34. Germany
35. Ghana
36. Greece
37. Grenada
38. Guatemala
39. Guyana
40. Haiti
41. Honduras
42. Hong Kong (City)
43. Hungary
44. Iceland
45. India
46. Iraq
47. Ireland
48. Israel
49. Italy
50. Jamaica
51. Japan
52. Jordan
53. Kenya
54. Kiribati
55. Latvia
56. Lesotho
57. Liberia
58. Liechtenstein
59. Lithuania
60. Luxembourg
61. Malawi
62. Malaysia
63. Malta
64. Mauritius
65. Mexico
66. Monaco
67. Myanmar (Burma)
68. Nauru
69. Nepal
70. Netherlands
71. New Zealand
72. Nicaragua
73. Nigeria
74. Norway
75. Pakistan
76. Panama
77. Papua New Guinea
78. Paraguay
79. Peru
80. Philippines
81. Poland
82. Portugal
83. Romania
84. St. Kitts & Nevis
85. St. Lucia
86. St. Vincent & the Grenadines
87. Seychelles
88. Sierra Leone
89. Singapore
90. Slovak Republic
91. Slovenia
92. South Africa
93. Spain
94. Sri Lanka
95. Suriname
96. Swaziland
97. Sweden
98. Switzerland
99. Tanzania
100. Thailand
101. Tonga
102. Trinidad & Tobago
103. Turkey
104. United Kingdom
105. Uruguay
106. Venezuela
107. Zambia

Appendix C – UN Membership As Of July 1999

With the admission of Palau, there are now 185 Member States of the United Nations. The Member States and the dates on which they joined the Organization are listed below:

1. Afghanistan -- (19 Nov. 1946)
2. Albania -- (14 Dec. 1955)
3. Algeria -- (8 Oct. 1962)
4. Andorra -- (28 July 1993)
5. Angola -- (1 Dec. 1976)
6. Antigua and Barbuda -- (11 Nov. 1981)
7. Argentina -- (24 Oct. 1945)
8. Armenia -- (2 Mar. 1992)
9. Australia -- (1 Nov. 1945)
10. Austria-- (14 Dec. 1955)
11. Azerbaijan -- (9 Mar. 1992)
12. Bahamas -- (18 Sep. 1973)
13. Bahrain -- (21 Sep. 1971)
14. Bangladesh -- (17 Sep. 1974)
15. Barbados -- (9 Dec. 1966)
16. Belarus -- (24 Oct. 1945)
17. Belgium -- (27 Dec. 1945)
18. Belize -- (25 Sep. 1981)
19. Benin -- (20 Sep. 1960)
20. Bhutan -- (21 Sep. 1971)
21. Bolivia -- (14 Nov. 1945)
22. Bosnia and Herzegovina -- (22 May 1992)
23. Botswana -- (17 Oct. 1966)
24. Brazil -- (24 Oct. 1945)
25. Brunei Darussalam -- (21 Sep. 1984)
26. Bulgaria -- (14 Dec. 1955)
27. Burkina Faso -- (20 Sep. 1960)
28. Burundi -- (18 Sep. 1962)
29. Cambodia -- (14 Dec. 1955)
30. Cameroon -- (20 Sep. 1960)
31. Canada -- (9 Nov. 1945)
32. Cape Verde -- (16 Sep. 1975)
33. Central African Republic -- (20 Sep. 1960)
34. Chad -- (20 Sep. 1960)
35. Chile -- (24 Oct. 1945)
36. China -- (24 Oct. 1945)
37. Colombia -- (5 Nov. 1945)
38. Comoros -- (12 Nov. 1975)
39. Congo -- (20 Sep. 1960)
40. Costa Rica -- (2 Nov. 1945)
41. Côte d'Ivoire -- (20 Sep. 1960)
42. Croatia -- (22 May 1992)
43. Cuba -- (24 Oct. 1945)
44. Cyprus -- (20 Sep. 1960)
45. Czech Republic -- (19 Jan. 1993)
46. Democratic People's Republic of Korea -- (17 Sep. 1991)
47. Democratic Republic of the Congo -- (20 Sep. 1960)
48. Denmark -- (24 Oct. 1945)
49. Djibouti -- (20 Sep. 1977)
50. Dominica -- (18 Dec. 1978)
51. Dominican Republic -- (24 Oct. 1945)
52. Ecuador -- (21 Dec. 1945)
53. Egypt -- (24 Oct. 1945)
54. El Salvador -- (24 Oct. 1945)
55. Equatorial Guinea -- (12 Nov. 1968)
56. Eritrea -- (28 May 1993)
57. Estonia -- (17 Sep. 1991)
58. Ethiopia -- (13 Nov. 1945)
59. Fiji -- (13 Oct. 1970)
60. Finland -- (14 Dec. 1955)
61. France -- (24 Oct. 1945)
62. Gabon -- (20 Sep. 1960)
63. Gambia -- (21 Sep. 1965)
64. Georgia -- (31 July 1992)
65. Germany -- (18 Sep. 1973)
66. Ghana -- (8 Mar. 1957)
67. Greece -- (25 Oct. 1945)
68. Grenada -- (17 Sep. 1974)
69. Guatemala -- (21 Nov. 1945)
70. Guinea -- (12 Dec. 1958)
71. Guinea-Bissau -- (17 Sep. 1974)
72. Guyana -- (20 Sep. 1966)
73. Haiti -- (24 Oct. 1945)
74. Honduras -- (17 Dec. 1945)

75. Hungary -- (14 Dec. 1955)
76. Iceland -- (19 Nov. 1946)
77. India -- (30 Oct. 1945)
78. Indonesia -- (28 Sep. 1950)
79. Iran (Islamic Republic of)-- (24 Oct. 1945)
80. Iraq -- (21 Dec. 1945)
81. Ireland -- (14 Dec. 1955)
82. Israel -- (11 May 1949)
83. Italy -- (14 Dec. 1955)
84. Jamaica -- (18 Sep. 1962)
85. Japan -- (18 Dec. 1956)
86. Jordan -- (14 Dec. 1955)
87. Kazakhstan -- (2 Mar. 1992)
88. Kenya -- (16 Dec. 1963)
89. Kuwait -- (14 May 1963)
90. Kyrgyzstan -- (2 Mar. 1992)
91. Lao People's Democratic Republic -- (14 Dec. 1955)
92. Latvia -- (17 Sep. 1991)
93. Lebanon -- (24 Oct. 1945)
94. Lesotho -- (17 Oct. 1966)
95. Liberia -- (2 Nov. 1945)
96. Libyan Arab Jamahiriya -- (14 Dec. 1955)
97. Liechtenstein -- (18 Sep. 1990)
98. Lithuania -- (17 Sep. 1991)
99. Luxembourg -- (24 Oct. 1945)
100. Madagascar -- (20 Sep. 1960)
101. Malawi -- (1 Dec. 1964)
102. Malaysia -- (17 Sep. 1957)
103. Maldives -- (21 Sep. 1965)
104. Mali -- (28 Sep. 1960)
105. Malta -- (1 Dec. 1964)
106. Marshall Islands -- (17 Sep. 1991)
107. Mauritania -- (7 Oct. 1961)
108. Mauritius -- (24 Apr. 1968)
109. Mexico -- (7 Nov. 1945)
110. Micronesia (Federated States of)-- (17 Sep. 1991)
111. Monaco -- (28 May 1993)
112. Mongolia -- (27 Oct. 1961)
113. Morocco -- (12 Nov. 1956)
114. Mozambique -- (16 Sep. 1975)
115. Myanmar -- (19 Apr. 1948)
116. Namibia -- (23 Apr. 1990)
117. Nepal -- (14 Dec. 1955)
118. Netherlands -- (10 Dec. 1945)
119. New Zealand -- (24 Oct. 1945)
120. Nicaragua -- (24 Oct. 1945)
121. Niger -- (20 Sep. 1960)
122. Nigeria -- (7 Oct. 1960)
123. Norway -- (27 Nov. 1945)
124. Oman -- (7 Oct. 1971)
125. Pakistan -- (30 Sep. 1947)
126. Palau -- (15 Dec. 1994)
127. Panama -- (13 Nov. 1945)
128. Papua New Guinea -- (10 Oct. 1975)
129. Paraguay -- (24 Oct. 1945)
130. Peru -- (31 Oct. 1945)
131. Philippines -- (24 Oct. 1945)
132. Poland -- (24 Oct. 1945)
133. Portugal -- (14 Dec. 1955)
134. Qatar -- (21 Sep. 1971)
135. Republic of Korea -- (17 Sep. 1991)
136. Republic of Moldova -- (2 Mar. 1992)
137. Romania -- (14 Dec. 1955)
138. Russian Federation -- (24 Oct. 1945)
139. Rwanda -- (18 Sep. 1962)
140. Saint Kitts and Nevis -- (23 Sep. 1983)
141. Saint Lucia -- (18 Sep. 1979)
142. Saint Vincent and the Grenadines -- (16 Sep. 1980)
143. Samoa -- (15 Dec. 1976)
144. San Marino -- (2 Mar. 1992)
145. Sao Tome and Principe -- (16 Sep. 1975)
146. Saudi Arabia -- (24 Oct. 1945)
147. Senegal -- (28 Sep. 1960)
148. Seychelles -- (21 Sep. 1976)
149. Sierra Leone -- (27 Sep. 1961)
150. Singapore -- (21 Sep. 1965)
151. Slovakia -- (19 Jan. 1993)
152. Slovenia -- (22 May 1992)
153. Solomon Islands -- (19 Sep. 1978)
154. Somalia -- (20 Sep. 1960)
155. South Africa -- (7 Nov. 1945)
156. Spain -- (14 Dec. 1955)
157. Sri Lanka -- (14 Dec. 1955)
158. Sudan -- (12 Nov. 1956)
159. Suriname -- (4 Dec. 1975)
160. Swaziland -- (24 Sep. 1968)

161. Sweden -- (19 Nov. 1946)
162. Syrian Arab Republic -- (24 Oct. 1945)
163. Tajikistan -- (2 Mar. 1992)
164. Thailand -- (16 Dec. 1946)
165. The former Yugoslav Republic of Macedonia -- (8 Apr. 1993)
166. Togo -- (20 Sep. 1960)
167. Trinidad and Tobago -- (18 Sep. 1962)
168. Tunisia -- (12 Nov. 1956)
169. Turkey -- (24 Oct. 1945)
170. Turkmenistan -- (2 Mar. 1992)
171. Uganda -- (25 Oct. 1962)
172. Ukraine -- (24 Oct. 1945)
173. United Arab Emirates -- (9 Dec. 1971)
174. United Kingdom of Great Britain and Northern Ireland -- (24 Oct. 1945)
175. United Republic of Tanzania -- (14 Dec. 1961)
176. United States of America -- (24 Oct. 1945)
177. Uruguay -- (18 Dec. 1945)
178. Uzbekistan -- (2 Mar. 1992)
179. Vanuatu -- (15 Sep. 1981)
180. Venezuela -- (15 Nov. 1945)
181. Viet Nam -- (20 Sep. 1977)
182. Yemen -- (30 Sep. 1947)
183. Yugoslavia -- (24 Oct. 1945)
184. Zambia -- (1 Dec. 1964)
185. Zimbabwe -- (25 Aug. 1980)

Source: UN Press Release ORG/1190 (15 Dec. 1994)

Selected References

Arkin, William M. "A Mouse that Roars?" Special to *washingtonpost.com*, June 7, 1999, <http://www.washingtonpost.com/wp-srv/national/dotmil/arkin.htm>.

Arquilla, John and David Ronfeldt, editors. *In Athena's Camp.* Santa Monica: Rand, 1997.

Bell, J. Bowyer. "Aspects of the Dragonworld: Covert Communications and the Rebel Ecosystem" *International Journal of Intelligence and Counterintelligence* 3.1 (1989): 15-43.

Byman, Daniel. "The Logic of Ethnic Terrorism." *Studies in Conflict and Terrorism* 21 (1998): 149-169.

Center for Strategic and International Studies (CSIS) Task Force Report. *The Nuclear Black Market.* Washington, D.C.: Center for Strategic and International Studies, 1996.

Constantini, P. *Virtual Armies Clash by Net.* LEXUS/NEXIS: Inter Press Service, 4 June 1996.

Crenshaw, Martha. "How Terrorism Declines." *Terrorism and Political Violence* 3.1 (1991): 69-87.

Crenshaw, Martha. "The Logic of Terrorism: Terrorist Behavior as a Product of Strategic Choice." In *The Origins of Terrorism*, edited by Walter Reich, 7-24. Washington, D.C.: Woodrow Wilson Center Press, 1990.

Crenshaw, Martha. "The Causes of Terrorism." *Comparative Politics* (July 1981).

Crenshaw, Martha, "An Organizational Approach to Analysis of Political Terrorism." *Orbis: A Journal of World Affairs* 29.3 (1985): 465-488.

Crenshaw, Martha and John Pimlott, editors. *The Encyclopedia of World Terrorism.* Armonk: M.E. Shapre, 1997.

Daft, Richard L. *Organization Theory and Design*, 6th ed. Cincinnati: South-Western College Publishing, 1998.

Defense Science Board. *Report on Information Warfare Defense.* Washington, D.C.: GPO, 1996.

DeNardo, J. *Power in Numbers: The Political Strategy of Protest and Rebellion.* Princeton: Princeton University Press, 1985.

Denning, Dorothy. *Information Warfare and Security.* Reading: Addison –Wesley, 1998.

Elan, Ivan. "Does U.S. Intervention Overseas Breed Terrorism?" *Cato Institute Foreign Policy Briefing* #50, Dec. 17,1998.

Falkenrath, Richard A., Robert D. Newman, and Bradley Thayer. *America's Achille's Heel: Nuclear, Biological, and Chemical Terrorism and Covert Attack.* Cambridge: MIT Press, 1998.

General Accounting Office (GAO). *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk.* Washington D.C.: GAO, 1998

General Accounting Office (GAO). *Information Security – Computer Attacks At Department Of Defense Pose Increasing Risks.* (Washington D.C.: GAO, 1996).

Grenier, Larry E. Evolution and Revolution as Organizations Grow." *Harvard Business Review* 50 (1972): 37-46.

Hoffman, Bruce. *Inside Terrorism.* New York: Columbia University Press, 1998

Hoffman, Bruce. *Responding to Terrorism Across the Technological Spectrum.* Presented to the Fifth Annual Conference on Strategy at the US Army War College Carlisle Barracks, PA, 15 July 1994.

International Telecommunications Union (ITU). *Yearbook of Statistics 1999.* Geneva: ITU, 1999.

International Telecommunication Union, *Challenges to the Network Internet for Development,* 1999. Geneva: ITU, 1999.

Iuris, A. P. "Information Terrorism" *Terrorism: A Global Survey.* London: Janes Information Group, 1997.

Jenkins, Brian Michael. I*nternational Terrorism: The Other World War.* Santa Monica: RAND, 1985.

Joint Chiefs of Staff (JCS). *Joint Pub 6-0: Doctrine for Command Control, Communications, and Computer (C4) Systems Support to Joint Operations.* Washington D.C.: Department of Defense, 1995.

Laqueur, Walter. "Postmodern Terrorism." *Foreign Affairs* 75-5 (1996): 27-31.

Lockett, Charles. *We Bomb, Therefore We Are: The Evolution of Terrorist Group Life Cycles.* Thesis, Naval Postgraduate School, Monterey, CA. 1994.

Medd, Roger and Frank Goldstein. "International Terrorism on the Eve of a New Millenium." *Studies in Conflict and Terrorism* 20 (1997): 281-316.

Mintzberg, Henry and James B. Quinn. *The Strategy Process.* 3rd ed. New Jersey: Prentice Hall, 1996.

Organization for Economic Co-operation and Development (OECD). *Information Technology Outlook 1997.*

Organization for Economic Co-operation and Development (OECD). *Working Party on Telecommunication and Information Services Policies,* Internet Infrastructure Indicators, 28 Oct 1988.

Post, Jerrold M. "Prospects for Nuclear Terrorism: Psychological Motivations and Constraints." In *Preventing Nuclear Terrorism*, edited by Paul Leventhal and Yonah Alexander. New York: Lexington Books, 1987.

Post, Jerrold M. "Terrorist Psycho-logic: Terrorist Behavior as a Product of Psychological Forces." In *The Origins of Terrorism*, edited by Walter Reich, 25-42. Washington, D.C.: Woodrow Wilson Center Press, 1990.

Post Jerrold M., "Narcissism and the Charismatic Leader-Follower Relationship." *Political Psychology.* 7.4 (1986): 675-687.

Post, Jerrold M, Kevin Rudy and Eric Shaw. *From Car Bombs to Logic Bombs: The Growing Threat from Information Systems Terrorism.* Washington D.C.: George Washington University, 1998.

Quinn, Robert E. and Kim Cameron, "Organizational Life Cycles and Shifting Criteria for Effectiveness: Some Preliminary Evidence." *Management Science* 29 (1983): 33-51.

Rattray, Gregory. *Information Warfare: Challenges for the United States.* Dissertation, Fletcher School of Law and Diplomacy, Tufts University, 1997.

Reich, Walter. *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*, edited by Walter Reich. Washington, D.C.: The Woodrow Wilson Center Press, 1990.

Robbins, Stephen P. *Organization Theory: Structure, Design and Applications,* 2nd ed. Englewood Cliffs: Prentice-Hall, 1987.

Schwartz, John, "Online Security Is Pentagon's Latest Battle." *Washington Post*, 2 June 1999, A2.

The President's Commission on Critical Infrastructure Protection. *Critical Infrastructures: Protecting America's Foundations.* Washington, D.C.: GPO, 1997.

The White House, Office of the Science and Technology Advisor. *Cybernation: The American Infrastructure in the Information Age.* Washington, D.C.: GPO, 1996.

United States Department of Defense. DoD O-2000.12-H.

United States Department of State. *Patterns of Global Terrorism: 1998.* Washington D.C.: GPO, 1999.

Wilson James Q. *Political Organizations.* New York: Basic Books, 1973.