LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

UCRL-TR-227068

Assessing Terrorist Motivations for Attacking Critical Infrastructure

G. Ackerman, P. Abhayaratne, J. Bale, A. Bhattacharjee, C. Blair, L. Hansell, A. Jayne, M. Kosal, S. Lucas, K. Moran, L. Seroki, S. Vadlamudi

January 4, 2007

This work was performed under the auspices of the U.S. Department of Energy by University of California, Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.

UCRL-TR-227068

Center for Nonproliferation Studies
Monterey Institute of International Studies

Assessing Terrorist Motivations for Attacking Critical Infrastructure

PREPARED BY:

The Weapons of Mass Destruction Terrorism Research Program

Center for Nonproliferation Studies
Monterey Institute of International Studies
460 Pierce Street
Monterey, California 93940

(831) 647-4154

Sponsor

Mary Beth Ward, Technical Project Monitor
International Assessments Program
Lawrence Livermore National Laboratory
Livermore, California

Funding

Science and Technology Directorate
U.S. Department of Homeland Security

Cover: The cover photo pictures the Tooele Chemical Agent Disposal Facility outside of Tooele, Utah in the evening. This public domain image is available at: http://ens.lycos.com/ens/sep2001/ 2001L-09-04-06.html.

"To build and implement a robust strategy to protect our critical infrastructures and key assets from further terrorist exploitation, we must understand the motivations of our enemies as well as their preferred tactics and targets."

The White House,
"The National Strategy for the Physical Protection of
Critical Infrastructures and Key Assets," 2003, p viii.

Center for Nonproliferation Studies

The Center for Nonproliferation Studies (CNS) strives to combat the spread of weapons of mass destruction (WMD) by disseminating timely information and analysis and training the next generation of nonproliferation specialists. CNS at the Monterey Institute of International Studies is the largest nongovernmental organization in the United States devoted exclusively to research and training on nonproliferation issues.

Dr. William Potter established the Center in 1989 with a handful of Institute students. Today, CNS has a full-time staff of more than 65 specialists and over 75 graduate student research assistants located in offices in Monterey, California, Washington, DC and Almaty, Kazakhstan. CNS is organized into five research programs: the Chemical and Biological Weapons Nonproliferation Program, the East Asia Nonproliferation Program, the International Organizations and Nonproliferation Program, the Newly Independent States Nonproliferation Program, and the WMD Terrorism Research Program (WMDTRP). Each program supports the Center's mission by training graduate students, building a worldwide community of nonproliferation experts, publishing both on-line and print resources on all aspects of WMD, providing background material to the media, and producing analysis for use by educational institutions, government, and the general public.

The WMD Terrorism Research Program conducts work on the use or potential use of chemical, biological, radiological and nuclear (CBRN) weapons by non-state actors. The Program focuses on the motivational aspects of terrorism in the WMD context, bringing together terrorism scholars from the social sciences (history and political science) and technical experts from the sciences (microbiology, medicine, chemistry, and physics) to approach the WMD terrorism problem in an interdisciplinary fashion.

Project Research Staff

***Principal Investigator*:**
Gary Ackerman, Director, WMDTRP

Investigators:
Praveen Abhayaratne, Research Associate, WMDTRP
Jeffrey M. Bale, PhD, Senior Research Associate, WMDTRP
Anjali Bhattacharjee, Research Associate, WMDTRP
Charles Blair, Research Associate, WMDTRP
Lydia Hansell, Graduate Research Assistant, WMDTRP
Andrew Jayne, Graduate Research Assistant, WMDTRP
Margaret Kosal, PhD, Post Doctoral Fellow, CBWNP
Sean Lucas, Graduate Research Assistant, WMDTRP
Kevin S. Moran, Research Associate, WMDTRP
Linda Seroki, Graduate Research Assistant, WMDTRP
Sundara Vadlamudi, Research Associate, WMDTRP

Support Staff:
Joel Baker, Graduate Research Assistant, WMDTRP
Erin Fitzpatrick, Graduate Research Assistant, WMDTRP
Lauren Harrison, Graduate Research Assistant, WMDTRP
Robert Wesley, Graduate Research Assistant, WMDTRP

TABLE OF CONTENTS

BOXES, FIGURES AND TABLES REFERENCED IN REPORT

Boxes

Figures

Tables

EXECUTIVE SUMMARY*

"To build and implement a robust strategy to protect our critical infrastructures and key assets from further terrorist exploitation, we must understand the motivations of our enemies as well as their preferred tactics and targets."

2003 National Strategy for the Physical Protection of Critical Infrastructures and Key Assets[1]

Project Overview

Certain types of infrastructure – critical infrastructure (CI) – play vital roles in underpinning our economy, security and way of life. These complex and often interconnected systems have become so ubiquitous and essential to day-to-day life that they are easily taken for granted. Often it is only when the important services provided by such infrastructure are interrupted – when we lose easy access to electricity, health care, telecommunications, transportation or water, for example – that we are conscious of our great dependence on these networks and of the vulnerabilities that stem from such dependence.

Unfortunately, it must be assumed that many terrorists are all too aware that CI facilities pose high-value targets that, if successfully attacked, have the potential to dramatically disrupt the normal rhythm of society, cause public fear and intimidation, and generate significant publicity. Indeed, revelations emerging at the time of this writing about al Qa'ida's efforts to prepare for possible attacks on major financial facilities in New York, New Jersey, and the District of Columbia remind us just how real and immediate such threats to CI may be. Simply being aware that our nation's critical infrastructure presents terrorists with a plethora of targets, however, does little to mitigate the dangers of CI attacks. In order to prevent and preempt such terrorist acts, better understanding of the threats and vulnerabilities relating to critical infrastructure is required.

The Center for Nonproliferation Studies (CNS) presents this document as both a contribution to the understanding of such threats and an initial effort at "operationalizing" its findings for use by analysts who work on issues of critical infrastructure protection. Specifically, this study focuses on a subsidiary aspect of CI threat assessment that has thus far remained largely unaddressed by contemporary terrorism research: the motivations and related factors that determine whether a terrorist organization will attack critical infrastructure. In other words, this research investigates: 1) why terrorists choose to attack critical infrastructure rather than other targets; 2) how groups make such decisions; 3) what, if any, types of groups are most inclined to attack critical infrastructure targets; and 4) which types of critical infrastructure terrorists prefer to attack and why.

In an effort to address the above questions as comprehensively as possible, the project team employed four discrete investigative approaches in its research design. These include:

- *a review of existing terrorism and threat assessment literature* to glean expert consensus regarding terrorist target selection, as well as to identify theoretical approaches that might be valuable to analysts and decision-makers who are seeking to understand such terrorist group decision-making processes;

* The Executive Summary was prepared by Kevin S. Moran.

[1] The White House, "The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets," 2003, p viii.

- *the preparation of several concise case studies* to help identify internal group factors and contextual influences that have played significant roles in leading some terrorist groups to attack critical infrastructure;

- *the creation of a new database* – the Critical Infrastructure Terrorist Incident Catalog (CrITC) – to capture a large sample of empirical CI attack data that might be used to illuminate the nature of such attacks to date; and

- *the development of a new analytical framework* – the Determinants Effecting Critical Infrastructure Decisions (DECIDe) Framework – designed to make the factors and dynamics identified by the study more "usable" in any future efforts to assess terrorist intentions to target critical infrastructure.

Although each is addressed separately in the following chapters, none of the four aspects of this study were developed in isolation. Rather, all the constituent elements of the project informed – and were informed by – the others. For example, the review of the available literature on terrorist target selection made possible the identification of several target selection factors that were both important in the development of the analytical framework and subsequently validated by the case studies. Similarly, statistical analysis of the CrITIC data yielded measurable evidence that supported hypotheses derived from the framework, the case studies, and the writings of various experts. Besides providing an important mechanism of self-reinforcement and validation, the project's multifaceted nature made it possible to discern aspects of CI attack motivations that would likely have been missed if any single approach had been adopted.

Defining the Issue

Given the lack of a clear, standard definition for "critical infrastructure" in contemporary policy discussions, this study reviewed all major existing U.S. Government definitions of the term and then crafted the following:

> **Critical infrastructures are those physical systems that a community depends on to maintain its security, governance, public health and safety, economy and public confidence. The constituent parts of such systems will vary according to the community context in which they are viewed.**

This intentionally broad definition was selected to depict the full scope of the concept as it is used by officials at the local, state, and national levels. It reflects three particularly important aspects of critical infrastructure that have been suggested in alternative definitions; namely:

- *critical infrastructure involves a vast and diverse set of assets that vary from community to community* – while standard examples of such systems exist – agriculture, power, telecommunications, transportation, and water, for example – it is difficult to classify CI into discrete categories because: 1) similar systems can be comprised of many different constituent parts (consider, for example, the differences between rural and urban critical infrastructures); and 2) new categories of CI can emerge and existing categories can shift, especially as technologies and system relationships change;

- *not all critical infrastructures are similarly "critical"* – CI is, by its nature, related to systems and services that are essential to the functioning of normal life. It is important to recognize, however, that what is deemed "essential" will vary depending on the level of the community concerned; consequently, local, state, and national perceptions of CI will vary. Where local communities might be concerned with the functioning of schools as a part of its CI, a national community would likely be more concerned with the security of its defense industrial base;

- all aspects of critical infrastructure can be broadly recognized as either "physical" (meaning tangible) or "cyber" (meaning virtual and information oriented) targets – acknowledging this distinction and the fact that both the characteristics and perpetrators of "cyber" and "physical" attacks often differ markedly from one another, *this study focuses exclusively on matters relating to "physical" critical infrastructure target selection*. Terrorist motivations relating to "cyber" CI issues are equally important, but are outside the scope of this study and warrant a separate investigation.

Literature Assessment

To ground this effort firmly in the foundations of existing terrorism and threat assessment research, more than 150 sources relating to critical infrastructure, terrorism, and risk analysis – including government reports, conference presentations, private and quasi-public sector analyses, and scholarly books and articles – were surveyed at the outset of the project. The review confirmed initial expectations that little to no existing work focuses specifically on the reasons why terrorists choose to attack critical infrastructure targets. Surprisingly, the review also revealed a paucity of material regarding the more general process of target selection by terrorist groups. While this discovery enabled our research to be conducted without the preexisting assumptions that sometimes encumber research, it also meant that the literature reviewed was of more value for framing than directly informing the issues at the heart of our study.

Most significantly, the literature helped identify key factors that are widely accepted by outside experts as being influential in shaping terrorist actions. These include:

- *factors related to the nature of the group*, specifically: Ideology; Organizational Structure; Organizational Dynamics; Organizational Lifecycle status (a terrorist group's maturity); Demographics; Resources; and Operational Capabilities;

- *factors external to the group,* specifically: Historical Context, Events, and Precedents; Relations with External Actors (such as sympathizers and supporters, the mass media, the general public, other extremist and criminal groups, and the state apparatus); the Security Environment; and Critical Infrastructure (target) Characteristics; and

- *decision-making factors*, specifically: General Planning Characteristics (such as decision-maker time horizons and risk thresholds); Perceptual Filter (how decision-makers perceive information external to the group); Operational Objectives (what a terrorist group hopes to achieve from its attacks); and Attack Modalities (the methods and techniques a terrorist group employs to attack targets).

While these factors may not be the only ones that affect terrorist targeting decisions, they are the ones we deemed significant enough to focus on and include in the project's DECIDe Framework. A number of themes recur throughout the literature and offer particular insight as to why and how various factors may exert an impact on terrorist motivations for attacking CI. Among the more important conclusions drawn from the study's literature analysis are the following.

- *Ideology* provides the essential rationale for a terrorist group's targeting and identifies what its permissible range of targets is by: 1) identifying clearly who the enemy ("them") is; and 2) providing a clear explanation of why it is legitimate for members of the group ("us") to attack that enemy.

- *Organizational Structure,* in particular aspects such as group size and bureaucratic sophistication, are often correlated directly with an organization's levels of resources, capabilities, and functional specialization. Larger, more highly differentiated groups will be both more likely to consider and more capable of effectively conducting elaborate attacks, because: 1) they will generally be able to consider larger potential target sets; and 2) they will often have the wherewithal to conduct more sophisticated and resource intensive attacks.

- *Organizational Dynamics* have the potential to play important roles in setting target priorities. In particular, group leaders – especially if they are charismatic, authoritarian, or totalitarian in nature – may dominate their organization's decision-making processes and play decisive roles in target selection. Alternatively, groups that undergo schisms and factionalization may experience a broadening of their potential target sets as various factions compete for influence with rival factions by proposing increasingly "extreme" (i.e., more brutal and destructive) attacks.

- The *Organizational Lifecycle Status* of a terrorist group can sometimes be used to gain insight into its general behavior. For example, successive generations that arise within particular terrorist groups are sometimes *less idealistic and often display a greater capacity for violence*, which might well have an impact on their operational objectives and consequent target selection. Others demonstrate a propensity to degenerate into criminality, which would often preclude certain types of destructive acts. Still others eschew the more limited, organization-building actions of their forbearers and move toward the planning of mass-casualty, apocalyptic-style attacks.

- *Resources* act as natural limitations on the targets terrorist groups can successfully attack. However ambitious their targeting goals may be, groups with few means will simply be unable to achieve many of their desired outcomes unless they can gain access to adequate financial, physical, and logistical resources.

- *Operational Capabilities* also affect a group's choice of targets, since few groups are likely to select targets that they knowingly lack the ability to attack successfully. In terms of developing new capabilities, terrorists have tended to rely on tried-and-true weapons and tactics for the simple reason that they have worked well in the past and continue to work well. As countermeasures become more elaborate and sophisticated, however, terrorists are inevitably forced to expand their capabilities so that they can adopt new techniques and/or employ new, more destructive weapons. In that sense, there is an ongoing cycle of innovation, as those who seek to protect targets and those who seek to attack them try to outmaneuver one another.

- *Perceptual Filters* – the biases through which all receive and interpret information – are ubiquitous when it comes to decision-making. However, in the case of terrorist groups, which are often isolated, under varying levels of stress, and already have radical and violent outlooks, these features are believed to be especially prominent. Including the perceptual filter in assessments of terrorist motivations to attack specific types of targets can help to inform analysis by highlighting the impact of perception on terrorist decision making, and specifically on target selection.

- *Historical Context,* especially as framed by precedents and resonant prior events, influences terrorist behavior in important ways. No terrorist group emerges with an entirely blank slate, since its members have invariably internalized, adopted, or adapted and modified many pre-existing ideas. Similarly, no terrorist group is entirely unaware of the methods and tactics employed by prior or existing terrorist organizations, especially those that have operated within its own political, intellectual, ethnic, religious, or cultural milieu.

- *External Relations* necessarily affect a terrorist group's selection of targets, and frequently also the level of violence it decides to employ. To ensure that their acts of violence do not become meaningless or counterproductive, terrorists wishing to achieve specific effects with their attacks must carefully take into account the opinions of external actors when selecting targets. Specifically, they must take into account the reactions of their supporters and sympathizers, their potential constituents, other extremist groups in their area, sponsoring states (if they have them), and above all the target "enemy" audience.

- Although the general *Security Environment* might be expected to affect terrorist operations, including target selection, dedicated terrorists are rarely if ever likely to cease planning and launching attacks, no matter how tough the overall security environment becomes.

- *CI [Target] Characteristics* are among the most important factors in a terrorist group's decision to attack – or not attack – specific targets. The most important characteristics of an infrastructure target that tend to affect terrorist targeting are its: 1) level of protection; 2) whether or not it has a high profile (which is in part a function of how much attention the media has paid to it); and 3) its actual function. All things being equal, terrorists are more likely to select targets that are vulnerable. At the same time, they wish to attack functionally important, high-profile targets, the damage or destruction of which will be costly to society. The key decision-making factor is usually the relationship between a facility's vulnerability and its desirability as a target. Given the large number and wide range of potential targets, terrorists will tend to avoid heavily-fortified or heavily-protected targets, unless these have extraordinary significance, and instead attack more vulnerable targets.

- *General Planning Characteristics* such as time horizons and risk thresholds can provide important insight into a terrorist group's ability or willingness to attack certain targets. For example, specific ideological or operational objectives can have an obvious and direct effect on the decision maker's time horizon, in that certain of these objectives may be time-dependent. The degree of risk that a group is willing to take in order to conduct any single attack is also an important factor in the setting of operational objectives. All else being equal, the greater the risk tolerance of a group when planning an attack, the greater the intended scale of the attack is likely to be.

- *Operational Objectives* – including desired casualty levels, level of publicity sought, whether the target should be symbolic or instrumental, the type and extent of the reaction terrorists want to elicit from various audiences, expected secondary effects, and hoped for scale of effects – play an unambiguous role in targeting decisions. Typically a group's operational objectives are shaped in large part by its ideology. Other dynamics that sometimes play a role in shaping operational objectives include the need to produce attack results that boost group morale, serve to differentiate the group from other terrorist groups, or demonstrate leadership will and commitment (this may be especially needed if a group is faced with factionalization).

- *Attack Modalities* are determined generally by the nature of the target itself, although the range of those modalities is limited to some extent by the existing capabilities and methods of the group. In some situations, however, a group may select a specific target because it is particularly well suited to an attack in which certain predetermined weapons or tactics can be used. This might be especially true of attacks that involve chemical or biological agents, which can be deployed effectively only in certain environments.

Case Studies

To shed further light on why certain types of terrorist groups might be more inclined to target CI than others, this study prepared a number of analyses of specific groups that have conducted major attacks against infrastructural targets. The groups examined in these analyses – the Jaish-e-Mohammed (JEM: Army of Mohammad) and Lashkar-e-Tayyiba (LET: Army of the Righteous), the Front de Liberation Nationale de la Corse (FLNC), Chukaku-ha, and the Moro Islamic Liberation Front (MILF) – are far from representative of the full universe of terrorist groups. They do, however, provide important insight – insight that is often impossible to obtain by means of quantitative research methods – into the motivations shaping the target selection of an ideologically and geographically diverse set of terrorist groups. Broadly speaking, the conclusions drawn from an examination of these "real life" cases complement and are consistent with the findings from the study's literature assessment and CrITIC. Several factors, in particular, should be highlighted as having played particularly important roles in influencing CI target selection in the cases considered. These include (in alphabetical order): CI Characteristics; External Relations; Factionalization; Historical Events; Ideology; Innovation; Knowledge of CI; Operational Objectives; Organizational Structure ; and Security Environment. A brief comment regarding each of these factors clarifies how these case studies helped further refine this study's understanding of terrorist motivations relating to CI attacks.

- *CI Characteristics*, in particular the symbolic nature and functional importance of such targets, appear to figure prominently in target selection as demonstrated in the case study regarding the JEM/LET attack on the Indian Parliament in 2001. This same case, however, also highlights the important long-term methodological challenge of categorizing terrorist attacks as "critical infrastructure attacks." Terrorists generally have multiple motives for attacking targets. In the case of CI attacks, interfering with the operations of a vital infrastructure may be of secondary importance compared to other motives such as traumatizing a population psychologically or killing large numbers of people.

- In the cases considered, *External Relations* clearly play an important role in the process of target selection. Chukaku-ha's avowed support for Japanese farmers and union members and the group's decision to champion certain issues relating to these constituencies affected its target selection more significantly than any other single factor. Similarly, the targets selected by the FLNC and MILF reflect, respectively, their commitment to the advancement of the rights of indigenous Corsicans and Moros. While external relations appear to impact target selection directly, it is impossible to generalize how such relationships will impact critical infrastructure targeting without undertaking a careful analysis of the specific groups, constituencies, and issues involved in each particular case.

- Although far from conclusive, several of the case studies suggest that *Factionalization* may impact target selection. In particular, autonomous, localized cell structures and competitive inter-cell dynamics, such as those found in the FLNC, might make groups more willing to pursue attacks that involve greater violence or have more severe consequences. Similarly, intense competition between rival groups sharing similar but distinct ideologies, as in the case of Chukaku-ha, might encourage groups to engage in particularly "spectacular" attacks designed to generate high levels of publicity and prestige. While some CI targets may be particularly well suited to achieve such ends – especially because of their "critical" nature – there are certainly other types of attacks that might likewise be conducted to achieve such aims.

- *Historical Events*, especially methodological precedents, are likely to be key factors in target selection. The MILF's tactic of attacking power grids, for example, was not novel. At least three other groups that the MILF was clearly aware of – the Communist New People's Army (NPA), the MNLF, and the Abu

Sayyaf Group – had conducted similar attacks. It is likely that the MILF efforts were at least in part informed by such precedents.

- *Ideology* appears to be one of the single most significant factors in influencing a terrorist group's target selection. In the case of the FLNC, for example, the organization's ideology created the parameters for its *Operational Objectives* and helped determine the categories of targets that it attacked. Generally speaking, the FLNC has sought to minimize casualties and focus its efforts on infrastructure-type targets. As a direct consequence, although it has conducted hundreds of attacks, the group appears to have intentionally killed fewer than fifty people between 1975 and 1995. In a similar fashion, Chukaku-ha's Trotskyist ideology appears to have influenced its target selection by emphasizing violent forms of protest against targets that symbolically represent "the systems" against which the group is fighting, or which are directly related to its struggle to champion workers' rights. MILF's ideology also appears to have restricted its target selection to non-Muslims and its less-religious Muslim rivals.

- A group's *Propensity to Innovate* appears to be an important factor related to its ability to consider new and unprecedented targets and to identify effective and novel types of attacks that may have a greater likelihood of success. Chukaku-ha's initial attack on the Japanese National Railway system, for example, was unprecedented in scope and implementation, which may have been one of the reasons for its success. (This may be especially true, considering that the group's successive attacks on the system were less effective, because Japanese officials were better prepared to deal with such contingencies.) Similarly, JEM was the first group to introduce *fidayeen*-style attacks in Jammu and Kashmir. The group had carried out a successful attack against the Kashmir State Assembly in 2001, and attempted to replicate the same tactic with less effectiveness in the Indian Parliament attack.

- In several of the case studies, group *Knowledge of CI* played a particularly important role in target selection and attack implementation. In the case of the JNR attack, it is clear that Chukaku-ha's detailed knowledge of the rail system allowed it to damage its target with maximum effectiveness. Indeed, it might be assumed that the group's prior knowledge of CI was the critical factor that enabled it to conceptualize the attack. While the FLNC and MILF attacks were simpler in nature, their knowledge of their targets and the environments in which the targets were located clearly influenced how they went about making their attacks and maximizing their impact.

- *Operational Objectives* unquestionably play a significant role in target selection. The FLNC is, perhaps, the most obvious example of the way in which operational objectives largely restricted the group's set of preferred targets to those involving physical assets such as CI. Since the FLNC's primary objective was to preserve their unique culture and establish effective political and economic control over their homeland, they focused most of their attacks on targets that were seen as perpetuating the second-class status of the native Corsicans. Chukaku-ha's attacks on JNR facilities were also likely designed to fulfill its operational objectives of raising public awareness of the Japanese government's efforts to privatize the rail system. Indeed, Chukaku-ha's highly successful 1985 attack directly affected approximately eleven million people and made them painfully aware of the group's issues.

- *Organizational Structure* appears to affect a terrorist group's capability to attack various critical infrastructure targets, but it is unclear that it increases a group's propensity to specifically attack CI. Chukaku-ha's large size and cell-based structure, for example, provided it with the manpower, operational capabilities and operational security necessary to conduct highly effective guerrilla acts that were especially successful against widely dispersed CI targets such as the Japanese rail system.

- The MILF's attacks against electrical infrastructure in the southern Philippines underscore the influence that the general *Security Environment* can have on motivating terrorist groups to undertake attacks against CI. These MILF attacks were a clear response to the Philippine Army's "Pikit Offensive," which was designed to overrun and destroy the MILF's Camp Buliok. The attacks against Mindanao's power grid were widely considered to be counterstrikes in response to this military offensive. Certain FLNC attacks against CI targets also appear to have been timed to respond to police efforts against the group.

CrITIC

Cognizant of the lack of existing open-source empirical data concerning critical infrastructure attacks available for quantitative analysis, CNS created CrITIC, the Critical Infrastructure Terrorist Incident Catalog. This unique database is populated by 1,874 incidents, all of which involve critical infrastructure attacks. (Of these, 188 have been identified as major CI attacks and 765 as minor CI attacks.) CrITIC's large data set, expansive time-frame – the incidents range chronologically from November 1933 to March 2004 – and carefully designed information fields make the database the only tool of its kind for conducting reliable "large N" analyses of CI attacks. While CrITIC remains a "work in progress" that will benefit significantly from additional refinement, further incident identification, and the clarification of cases lacking sufficient information, the database is already valuable for enhancing understanding of the historic trends of critical infrastructure attacks conducted by terrorists. Several major trends, in particular, should be highlighted:

- *CI attacks have increased significantly since the 1960s.* The number of CI attacks that could be "attributed" to specific perpetrators increased from only 42 in the decade of the 1960s to 116 in the 1970s to 471 in the 1980s. It decreased to 308 in the 1990s and now stands at 131 for the first three and one half years of the new millennium. In short, there has been, roughly, a ten-fold increase in the total number of CI attacks from the decade of the 1960s to that of the 1990s. While these numbers may indicate that terrorists are developing a growing interest in attacking CI, further analysis comparing the increases in CI attacks to the overall increases in all terrorist activity during the last several decades is required before more definitive conclusions can be drawn.

- *Energy and Government-related facilities have been the most commonly attacked CI targets. O*f the attributable major CI attacks between 1933 and 2003, oil, gas, power and government facilities were targeted most frequently. If one considers minor attacks against CI, attacks against embassies and consulates accounted for nearly 50% of the attacks.

- *To date, a majority of all CI attacks involve bombings.* Up until now, bombings (of all types) appear to be the most favored method of attacking CI. Of the 188 major attacks conducted by known perpetrators, 112 involved various types of bombs. When both major and minor CI attacks are considered, more than 60% of the incidents involved bombs. Following bombings, sabotage is the most common tactic used in major CI attacks. When minor attacks are included, projectiles such as mortars and rocket-propelled grenades constitute the second most frequent method of attack.

- *Terrorist groups of a "religious" nature are perpetrating a growing number of CI attacks.* Noticeable shifts in the proportion of CI attacks conducted by different types of terrorist groups are apparent over the last several decades. During the 1960s, most CI attacks were carried out by Ethno-Nationalist groups and by Secular Utopian groups. Religious groups were responsible for only a single CI attack during this period. In the 1970s, the pattern shifted slightly. Secular Utopian groups were responsible for 40 CI attacks, Ethno-Nationalist groups for 12, and Religious groups for only one. While this same pattern held generally during the 1980s and 1990s – Secular Utopian groups were responsible for 161 and 62 CI

attacks, respectively, and Ethno-Nationalist groups for 80 and 46 – Religious groups significantly increased their CI attacks, conducting 32 (7%) identifiable attacks in the 1980s and 51 (10%) in the 1990s. During the first three years of the new millennium, CI attacks attributable to Religious groups total 26 (20%) CI attacks, as compared to 30 (23%) by Secular Utopian groups and 11 (8%) by Ethno-Nationalist groups. In other words, Religious groups are now among the most prolific of all terrorist group types in carrying out CI attacks.

- *Left-Wing and Islamist groups attack CI more frequently than other types of groups.* Left-Wing groups (above all Marxist-Leninist groups) carried out the overwhelming majority of attacks attributable to groups that fall within the Secular Utopian category, as opposed to Anarchist, Neo-Fascist, or Ecological groups. Similarly, Islamist groups were responsible for carrying out the majority of CI attacks that have been perpetrated by Religious groups in the past two decades. Between 1980 and 2004 Religious groups were responsible for 89 incidents, of which Islamist groups were responsible for 84 or 94%.

- *Secular Utopian and Religious groups are responsible for a majority of recent CI attack fatalities.* Secular Utopian and Religious groups are the most deadly groups, with the latter being responsible for 80% of the casualties from attributable major attacks and 35% of the fatalities in the same category. This seems to reflect general terrorism attack trends involving Religious terrorist groups. These statistics suggest that Religious groups may be more likely than other groups to mix CI attacks with mass casualty attacks. In contrast, of the seven most historically active terrorist groups in terms of CI attacks – the IRA, the ETA, FARC, Shining Path, the ASALA, the FLNC, and the RAF—none is identified in the database as having killed more than four people in a single CI attack.

DECIDe Framework

This study was undertaken to develop a greater understanding of the factors and dynamics that induce terrorists to attack critical infrastructure. Perhaps more importantly, it was designed to "operationalize" the resulting research in a form that might enable analysts and policymakers to better mitigate future threats to CI. It was with this ultimate objective in mind that the Determinants Effecting Critical Infrastructure Decisions (DECIDe) Framework was developed as a tool to evaluate the likelihood that certain terrorist groups might attack various types of critical infrastructure. (See Chapter 5 for a full explanation of the framework and the process by which it can be used.)

The DECIDe Framework is based on a "contributing factors approach" that: 1) lays out the key elements (factors) that shape a terrorist group's targeting decision; 2) indicates the major relationships and interplay between these factors; and 3) makes clear their direct influences on target selection. (See Figure ES-1.) The factors and sub-factors used in the framework, as well as the relationships between them, are based upon the conclusions and hypotheses drawn from the literature assessment, case studies and data analysis discussed previously.

As should be clear from the factor diagram, the DECIDe Framework is dynamic in many respects, especially since influences on decisions can circulate through several factors – and then back again – in the process of contributing to decision-making. At this stage of the framework's development, however, the actual decision is regarded as single event-focused and monadic. This means that the framework represents a "one-shot"' process – the group is considering a single attack, as opposed to a long-term campaign. Therefore, although the decision-maker may take into account the reactions of external actors (such as the response of the public or the terrorists' constituency), these actors are not regarded at this stage as decision-making entities in their own right, and their decision-making processes are not captured in the framework. Nonetheless, the framework presented here can still serve as a powerful tool (and an improvement over existing methods) by capturing the most important dynamics of target selection, especially when considering terrorist groups with short planning horizons or "ad-

hoc" groups that coalesce for the purposes of conducting a single attack, such as the group responsible for the first World Trade Center bombing in 1993.

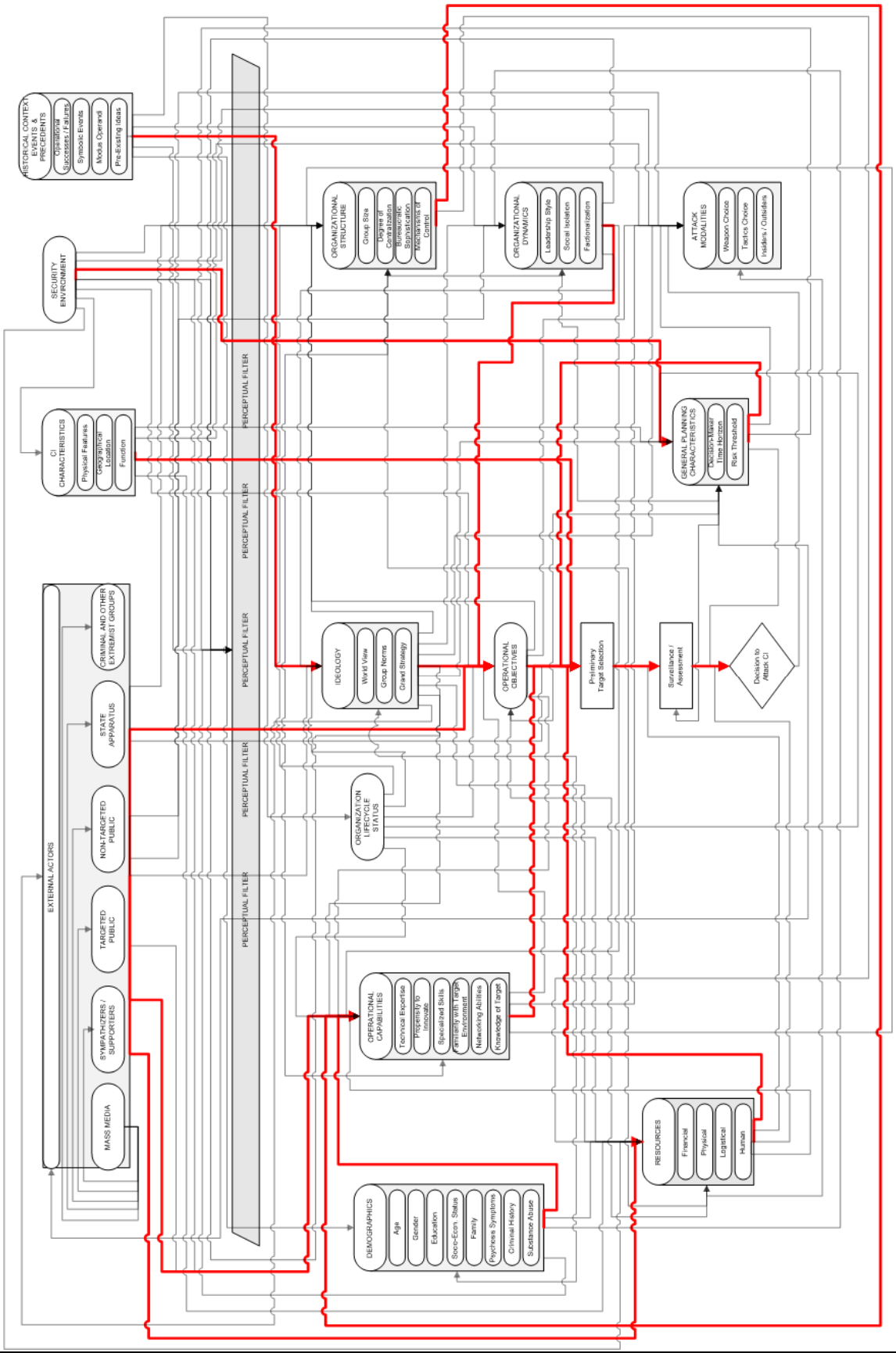


Figure ES-1: Contributing Factors Diagram

While the DECIDe Framework constitutes an important first step toward developing an analytical tool that can be reliably used to help discern terrorist motivations for attacking CI, much work remains to be done before it is ready for "field" deployment. At this stage, the framework remains both overly complex and too cumbersome to be used easily. While its present iteration may be sufficient for a theoretical investigation such as this, in which all background information is vital, the model is not yet "user-friendly." Additionally, although the hypothetical factor relationships included in the framework are held with a high degree of confidence by the project team, they deserve additional investigation and validation to ensure that the framework is as reliable as possible. Finally, the framework itself requires testing, validation, and iterative improvement – ideally in a process that involves both users and developers.

Integrating the Research Streams

Based on the motivational factors identified in the case studies and literature assessment, the trends suggested by CrITIC data, and preliminary analysis based on the DECIDe Framework it might be expected that the groups that are currently most likely to carry out attacks on U.S. infrastructure fall into three main categories: 1) Islamist terrorist groups – especially those with a global agenda; 2) domestic right-wing "militias" – in particular those that bitterly oppose both the "New World Order" and the "Zionist Occupation Government," which they believe has usurped power in the U.S.; and 3) violent fringes of the radical ecology movement – especially those with an uncompromising anti-technology or neo-Luddite agenda (e.g., philosophical "primitivists" and the most extreme proponents of the mystical, technophobic, and anti-rationalist "deep ecology" current). Finally, certain violence-prone groups that have attached themselves to the worldwide and extraordinarily diverse "anti-globalization" movement, in particular small but violent anarchist and neo-fascist factions, may eventually constitute an infrastructural threat. There are a number of indications that these are the milieus from which the greatest danger stems.

Next Steps

For an area of terrorism study as vital as target selection, it is surprising that so little qualitative *or* quantitative research has been focused specifically on how terrorists make targeting decisions. This study attempts to fill this inexplicable research gap, primarily by demonstrating the type of results that can be achieved through the simultaneous utilization of a number of parallel approaches in the examination of terrorist motivations for attacking CI. Despite the study's significant findings, the project team has identified a number of areas that could benefit from further investigation and development. Such additional efforts would serve to broaden and deepen our understanding of terrorist motivations for attacking CI, as well as refine the study in ways that would make it both more accessible and useful to the policy, security, and research communities. Three aspects of the project, in particular, should be highlighted as areas that offer opportunities for valuable future development:

- *Case Studies.* As has been demonstrated by the cases included in this report, qualitative case studies are uniquely well-suited to enhancing our understanding of the significant – but frequently difficult to observe and quantify – factors and dynamics that influence terrorist decision making. Additional examination of primary and secondary sources – such as ideological treatises, brochures, and communiqués that have been published and disseminated by particular terrorist groups; internal documents produced by those groups, such as bulletins, instructions, or the summaries of strategy sessions that have been recovered as a result of law enforcement or other research activities; intelligence documents and judicial materials concerning the activities of these groups; and interviews with former members of the groups – would provide far greater insight into the decision-making processes of terrorist groups, including in the context of CI targeting.

- *Database.* CNS' CrITIC database is likely the most robust – and possibly *only* – database exclusively designed to collect information about terrorist attacks on critical infrastructure. Although reasonably comprehensive, CrITIC is still in its early stages of development and can be further improved to provide more accurate and informative data and analysis. Four near-term tasks would be particularly valuable: 1) confirm the validity of CrITIC by investigating all identified incidents further; 2) conduct additional research into incidents lacking sufficient information to resolve ambiguities and enhance CrITIC's dataset; 3) use advanced statistical techniques – including logit and probit models – to assess the interplay and relative significance of each variable with greater accuracy; and 4) update CrITIC with new CI terrorism incidents on an ongoing basis.

- *Framework.* As noted previously, the DECIDe Framework is not "user-friendly" in its current form. We feel that an urgent next step is to convert the current framework into a more streamlined product, preferably one that is presented in an interactive computer-based format. Given that the theoretical underpinnings of the framework have already been established, its transition from paper to PC should be a fairly straightforward exercise. It is also notable that the framework still contains a number of hypotheses that require further validation. Additionally, since the existing framework is a "single shot" model that only focuses on terrorist motivations for discrete attacks, an important prospect for further research is to extend the model so that it can be used to evaluate longer term terrorist "campaigns."

This study is an important first step in demonstrating that there are useful ways to go about assessing the significant motivational element of the terrorist threat. We are confident that – especially as the process is improved and refined – continued use of this integrated multi-pronged research approach will yield further significant results in the field of terrorist behavior analysis that have long been unobtainable through strictly qualitative and quantitative efforts.

Chapter 1: INTRODUCTION*

It is no great surprise that concern about the security of our nation's critical infrastructure against terrorist attacks is growing. On the one hand, globalization and the often dizzying pace of technological advancement have resulted in a society that is increasingly connected, interdependent and therefore more vulnerable to intentional disruption than ever before.[2] At the same time, terrorists are displaying both the desire and the capability to cause greater death and destruction than they have in the past. Since one of the most effective ways for terrorists, as asymmetric combatants, to achieve the levels of publicity and intimidation they seek is to disrupt the normal rhythm of society, the assets upon whose continued functioning this rhythm depends have naturally become attractive targets for attack. Even as this research effort neared its completion, new revelations about al-Qa`ida's efforts to prepare for possible attacks on major financial facilities in New York, New Jersey, and the District of Columbia remind us just how real and immediate such threats may be.

Yet merely knowing that the nation's critical infrastructure presents our terrorist enemies with a plethora of targets does little to assuage our concern. In order to prevent and preempt such attacks, we require a full understanding of the threats, vulnerabilities and opportunities for recovery that pertain to critical infrastructure. CNS presents this study as a preliminary contribution to an understanding of the threat, at the same time offering an analytical framework that can quickly be adapted for use by analysts working on the problem of critical infrastructure protection.

The current study should be viewed in the context of a threat assessment, and as such some brief words about the general nature of threat assessment may help to situate the study within the broader category of evaluating threat and risk. The term "risk assessment" encompasses two main issues, chance and consequence. Chance refers to the likelihood that an undesirable incident will take place. Consequence refers to the results of such an event.[3] The term "threat assessment"[4] falls within the former category, while consequence management is part of the latter.

Threat assessment, the first step in any risk assessment program – including one related to critical infrastructure (CI) – concerns three interrelated facets: identifying the asset or class of assets on which to perform the assessment and determining the asset's value; that asset's vulnerability to attack; and the likelihood that it will be attacked. In the case of CI, such as an oil refinery, its value is not necessarily only its objective measurable worth. Rather, it is the asset's total value to those interested in protecting the asset from harm, including the political and social costs associated with disruption, which are often intangible measures.

---

* The introduction to this chapter was written by Gary Ackerman. Tthe CI Definitions section was written by Kevin S. Moran.

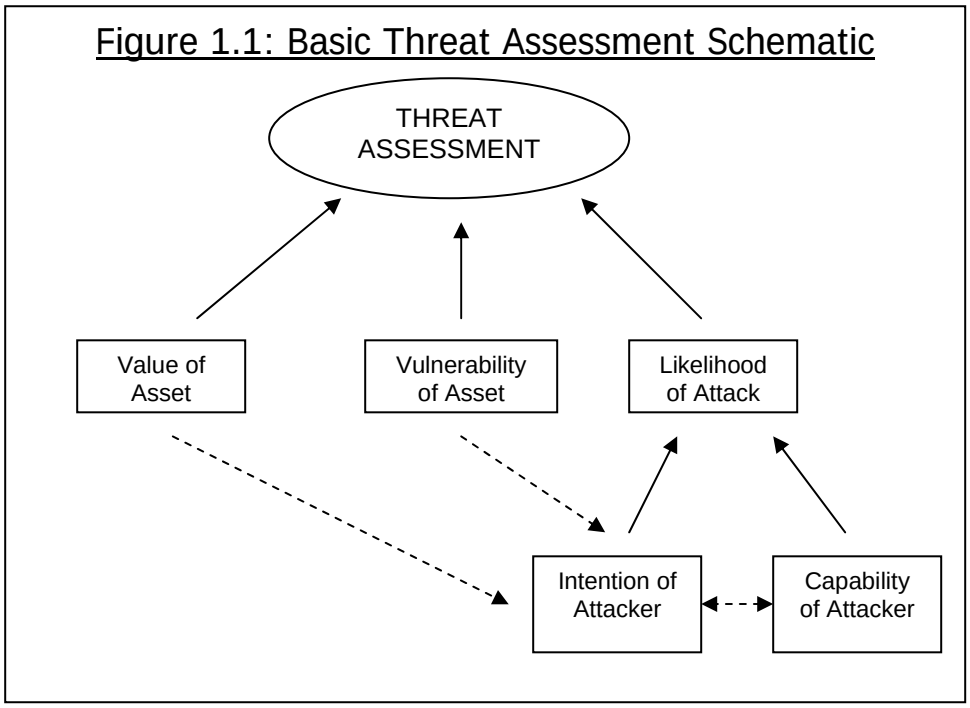
[2] Many examples of infrastructure in modern American society, such as the Internet and the air traffic system are structured as scale-free networks, a topology that, while resistant to random failures, is especially vulnerable to intentional attacks. For more on the vulnerability of different types of networks, see Albert-László Barabási, *Linked: The New Science of Networks* (Cambridge: Perseus Publishing, 2002).

[3] The other element of risk assessment, "consequence management," is not a focus of the current study.

[4] Any serious analysis of terms like "risk assessment" or "threat assessment" can easily become bogged down in a morass of definitions that various governmental and non-governmental entities employ for them. In short, there is no commonly accepted definition for a host of terms associated with risk assessment. For example, one Congressional study has defined "threat assessment" almost exclusively in terms of the capabilities of non-state actors to attack certain high-value targets (Rob Buschmann, "Risk Assessment in the Presidents National Strategy for Homeland Security," Congressional Research Service, October 31, 2002, pp. 1-2). In contrast, other threat assessment definitions have focused more on how a facility's attributes might increase a target's attractiveness in the eyes of an aggressor (Nancy A Renfroe and Joseph L. Smith. *Threat/Vulnerability Assessments and Risk Analysis. Whole Building Design Guide*. Accessed on 03/11/2004 at http://www/wbdg/org/design/res-print.php?rp=27). The current study therefore defines these as it uses them.

In contrast, vulnerability analysis – the second broad element of threat assessment – tends to be determined by more objective factors, such as the ease with which the target's perimeter can be breached. Related to both the value of the asset and its vulnerability is the third broad component of threat assessment: likelihood of attack. This component entails an analysis of who potential attackers might be, how likely they are to attack the asset, the determinants of their motivation to attack, and how capable they are of succeeding in an attack. Unfortunately, these factors are to a large extent dependent on the first two components, or more accurately, on the attacker's *perception* of the asset's value and vulnerability and their capability to exploit these. To attackers, the calculus used to determine value is often a subjective equation that includes the target's symbolic value and the psychological impact an attack upon it would have on a prospective target audience, whereas vulnerability becomes a function of how the attacker perceives the target's defenses. Figure 1.1 illustrates this structure, with dotted lines representing the attacker's perception.

Figure 1.1: Basic Threat Assessment Schematic



This aspect of threat assessment is therefore best undertaken after the "objective" value and vulnerability of the asset have been established, and in a sense is an amalgam of the subjective and objective elements of the two. It should be noted that most open-source threat analyses deal with value only implicitly or generically and instead emphasize the role of vulnerability. In those instances where the likelihood of attack is even considered, it is mostly in terms of the attacker's capabilities to attack, whereas the element of intent is often ignored. It would be hard to overemphasize the importance of including the motivations of potential attackers in the calculus of risk analysis. Unfortunately, the vast majority of risk analysis studies omit this critical component.[5] The reasons for this, no doubt, include the fact that the motivational aspects of threat assessment are exogenous and highly subjective factors which often fall into the realm of "soft" analysis.

[5] For examples of this exclusion, see U.S. General Accounting Office, "Combating Terrorism: Threat And Risk Assessments Can Help Prioritize and Target Program Investments;" GAO/NSIAD-98-74; Martz, Harry F. and Mark E. Johnson. "Risk Analysis of Terrorist Attacks," *Risk Analysis*. Vol.7 No.1 (1987); Renfroe, Nancy A, and Joseph L. Smith. "Threat/Vulnerability Assessments and Risk Analysis. Whole Building Design Guide". Accessed on 03/11/2004 at http://www/wbdg/org/design/res-print.php?rp=27; and Office for Domestic Preparedness (OPD), "Vulnerability Assessment Methodologies Report", U.S. Department of Homeland Security, Phase I Final Report, July 2003.

Neglecting the motivational aspects of threat assessment can result in sub-optimal outcomes, especially in the form of an inordinate focus on worst-case terrorism scenarios. Systematized, analytically sound threat assessments can temper these distortions and give both policymakers and the general public a sounder basis from which to address the issue, as well as allowing for more effective and wiser allocations of limited governmental resources.

Admittedly, assessing what drives a particular group to select a CI target over any of the myriad of alternatives is no easy task, so much so that some commentators almost despair about the possibilities of developing useful analyses in this area. As Robert Jervis once stated, "Judging others' intentions is notoriously difficult. Any number of methods of inference can be used, all of them fallible."[6] We must not, however, allow the best to be the enemy of the good – any tool that can assist us in determining which groups pose the greatest threat to critical infrastructure and why this is so, is valuable if it pushes the envelope of existing understanding.

A. Methodological Overview

The CNS project team embarked on the current study with alacrity, only to find this particular area of analysis largely devoid of existing content, at least in terms of the open sources. What tools did exist either did not address intent directly, or proposed a variety of threat assessment models that were felt to lack empirical and theoretical justification. In fact, the research team identified only a single comprehensive analytical source discussing target selection, that of Drake,[7] and although this work proved to be useful as a foundation for this study, it did not address the issue of critical infrastructure targets. In many respects, then, the current study could be said to have begun fresh, which offers the double-edged sword of being unencumbered by previous patterns of thinking but having very little guidance to follow.

In the end, three goals appeared to the project team to be paramount:

1) To accumulate as much data on critical infrastructure attacks as possible within the project time frame;
2) To leverage this data into analytical insights and formal knowledge; and finally
3) To convert this knowledge into a form that would be usable in a practical context.[8]

The project team developed four key research questions that guided all subsequent research efforts:

1) *Why would terrorists[9] attack Critical Infrastructure rather than other targets?*
2) *Which types of Critical Infrastructure do terrorists prefer to attack?*
3) *What types of groups or specific groups are most likely to attack Critical Infrastructure?*
4) *How do groups make decisions to attack Critical Infrastructure?*

A fifth question, namely "What attack methods (weapons systems, operational techniques etc.) are most likely to be used by groups in carrying out a Critical Infrastructure attack?" was also considered, although this question was not the focus of the project and will only be dealt with cursorily.

---

[6] Robert Jervis, "Perceiving and Coping with Threat," in Robert Jervis, Richard Ned Lebow and Janice Gross Stein, *Psychology and Deterrence* (Baltimore, MD: Johns Hopkins University, 1989), p. 14

[7] C.J.M Drake, *Terrorists' Target Selection* (New York: St. Martin's, 1998).

[8] See the introductory passages in Chapter 5 for the reasons we believed this to be important.

[9] While this study uses the term "terrorist" for convenience sake, all of its findings apply equally to other violence-prone non-state extremists. See the discussion of terrorism in Chapter 2.

In order to answer the above questions, the project team adopted a multifaceted research approach that included capturing a large sample of data on critical infrastructure attacks, conducting several in-depth case studies, reviewing the extant literature, and combining these results in the development of an analytical framework to assist in a determination of terrorist intentions to target critical infrastructure. The team remained fully aware that this work was exploratory and that much of it consisted of "feeling the topic out." Therefore, in the interests of transparency, this study is more meticulous than most in delineating the specific source of each observation, whether this be a researcher's hypothesis, a point derived from the literature, or information based on empirical evidence. Throughout this report, hypotheses developed by members of the project team are italicized and colored in red.

In addition, the following scheme is used to characterize assertions derived from the literature:

- 1 – Primary author assertion only
- 2 – Multiple authors' assertion
- 3 – Anecdotal evidence
- 4 – Theoretical evidence (e.g. derived from a game theoretic model or clinical study)
- 5 – Large *N* study (based on statistical data)

The highest degree of evidence present in each case is annotated.

The most important precursor to any analysis is a comprehensive understanding of the concept under study. Hence we must begin by examining the sometimes thorny definitional issues surrounding Critical Infrastructure.

B. Defining Critical Infrastructure

Public awareness of the vital roles that certain types of infrastructure play in underpinning our economy, security, and way of life has increased significantly during the last decade. This heightened attention has occurred at a time when our society has been shaped dramatically by the dynamics of information technology and the aftermath of 9/11. As notions of "networks" and "terrorism" have become more commonplace in popular culture, the U.S. government has reflected these developments by focusing its attention on issues relating to both the myriad of interconnected systems that make our day-to-day lives possible, as well as on the vulnerabilities that stem from such complex interactions and their resulting dependencies. In many ways, contemporary policy discussions regarding critical infrastructures are the 21st century corollaries to the heated "infrastructure" debates of the 1980s.[10] Then, as now with CI, "infrastructure" was a topic that involved numerous perspectives and opinions, but very few standard or agreed-upon definitions. "Infrastructure" was a fluid concept that could be used and interpreted in a wide variety of ways depending upon the policy context. Today, the same holds true for the term "critical infrastructure." In the absence of a clear, standard definition, this section seeks to identify the term's essential meaning by reviewing the major federal policies, reports, and actions that have framed how critical infrastructure is best understood in the context of current discussions relating to terrorism.

[10] A 2003 Congressional Research Service Report notes, "Nearly 20 years ago, infrastructure was debated because of concern that the nation's public works infrastructure was believed to be suffering from severe problems of deterioration, technological obsolescence, and insufficient capacity to serve future growth." See, John Moteff et al., "Critical Infrastructures: What Makes an Infrastructure Critical?" Congressional Research Service, January 29, 2003, p. 14.

Executive Order 13010. "Critical infrastructure" became an official term of public policy on July 17, 1996, when President Clinton signed Executive Order (EO) 13010 – Critical Infrastructure Protection, thereby establishing a joint public-private commission[11] to develop a national strategy "for protecting [critical infrastructures] and ensuring their continued operation."[12] Although the EO did not formally define the concept, it framed the idea by noting that "[c]ertain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."[13] More concretely, the EO identified the following specific infrastructures as critical:

> "telecommunications; electrical power systems; gas and oil storage and transportation; banking and finance; transportation; water supply systems; emergency services (including medical, police, fire, and rescue); and continuity of government."[14]

The language of the EO provides four important insights into early government thinking about the matter. First, it makes clear that the notion of critical infrastructure originated as a security concept. "Critical" infrastructures, according to the EO, are only those that have the potential to cause "debilitating" damage to the nation if they are harmed. Second, the EO carefully differentiates between two categories of threats posed to critical infrastructure. One set of threats – "physical threats" – involves attacks that impact an infrastructure's "tangible property." These are the types of threats addressed in this study. The other set – "cyber threats" – involves "electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures,"[15] and are not dealt with in the current study. Third, the EO offers an indication of the geographic scale on which critical infrastructure threats were initially evaluated. Only those infrastructures that have the potential to cause "regional" or "national" impact if harmed are addressed by EO 13010. And fourth, by emphasizing the private sector's important role in protecting CI, the EO makes clear that critical infrastructures are to be conceived of more broadly than the public goods that were usually considered as "infrastructure."

President's Commission on Critical Infrastructure Protection. In October 1997, the commission created by EO 13010 issued its final report.[16] Although it touches on both the physical and cyber threats to critical infrastructures, the bulk of the commission's report focuses on the potentially devastating risks posed to the nation by poor information security. To address this emerging challenge, the commission concluded that enhanced critical infrastructure protection was dependent on "industry cooperation and information sharing, a national organization structure, a revised program of research and development, a broad program of awareness and education, and reconsideration of laws related to infrastructure protection."[17] The commission also emphasized the difficulties inherent in accurately defining the nature of critical infrastructure, stating that CI "span a vast and diverse set of industries, technologies, people, and traditions."[18] In an effort to "convey a common understanding of critical infrastructures in the context" of its report, the commission used language taken from EO 13010 to define "critical infrastructures" as:

---

[11] The commission was officially titled the "President's Commission on Critical Infrastructure Protection."
[12] Executive Order *13010 – Critical Infrastructure Protection*. July 15, 1996, as found at: http://www.fas.org/irp/offdocs/eo13010.htm.
[13] *Ibid*.
[14] *Ibid*.
[15] *Ibid*.
[16] See: "Critical Foundations: Protecting America's Infrastructures," October 1997, as found at: http://www.dtra.mil/press_resources/publications/deskbook/full_text/Other_Relevant_References/PCCIP_Report.pdf
[17] General Accounting Office, "Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors," Report to the Committee on Energy and Commerce, U.S. House of Representatives, February 2003, p. 11.
[18] President's Commission on Critical Infrastructure Protection, "Critical Foundations: Protecting America's Infrastructures," October 1997, Appendix II, as found at: http://www.dtra.mil/press_resources/publications/deskbook/full_text/Other_Relevant_References/PCCIP_Report.pdf.

> "Infrastructures which are so vital that their incapacitation or destruction would have a debilitating impact on defense or economic security."[19]

Additionally, based on its own research and private sector input, the commission presented more detailed explanations of each of the critical infrastructures it addressed in its final document. (See Box 1.1.) These are the first formal government definitions that identify particular physical facilities that may be considered critical infrastructure. In addition to clarifying the nature of critical infrastructure, the commission's report provided further insight into the types of CI threats the government was concerned about. In particular, it noted that in terms of physical threats, the two most "critical" threats involve: "1) the targeting of key links and nodes whose destruction might ripple through infrastructures or across infrastructures; and 2) coordinated attacks which, in combination, could severely impact the nation's security and economic competitiveness."[20]

Box 1.1**

CRITICAL INFRASTRUCTURE DEFINITIONS FROM THE PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION

Banking and Finance: A critical infrastructure characterized by entities, such as retail and commercial organizations, investment institutions, exchange boards, trading houses, and reserve systems, and associated operational organizations, government operations, and support activities, that are involved in all manner of monetary transactions, including its storage for saving purposes, its investment for income purposes, its exchange for payment purposes, and its disbursement in the form of loans and other financial instruments.

Electrical Power Systems: A critical infrastructure characterized by generation stations, transmission and distribution networks that create and supply electricity to end-users so that end-users achieve and maintain nominal functionality, including the transportation and storage of fuel essential to that system.

Emergency Services: A critical infrastructure characterized by medical, police, fire, and rescue systems and personnel that are called upon when an individual or community is responding to emergencies. These services are typically provided at the local level (county or metropolitan area). In addition, state and Federal response plans define emergency support functions to assist in response and recovery.

Gas and Oil Production, Storage and Transportation: A critical infrastructure characterized by the production and holding facilities for natural gas, crude and refined petroleum, and petroleum-derived fuels, the refining and processing facilities for these fuels and the pipelines, ships, trucks, and rail systems that transport these commodities from their source to systems that are dependent upon gas and oil in one of their useful forms.

Information and Communications: A critical infrastructure characterized by computing and telecommunications equipment, software, processes, and people that support: the processing, storage, and transmission of data and information; the processes and people that convert data into information and information into knowledge; and the data and information themselves.

Transportation: A critical infrastructure characterized by the physical distribution system critical to supporting the national security and economic well-being of this nation, including the national airspace system, airlines and aircraft, and airports; roads and highways, trucking and personal vehicles; ports and waterways and the vessels operating thereon; mass transit, both rail and bus; pipelines, including natural gas, petroleum, and other hazardous materials; freight and long haul passenger rail; and delivery services.

Water Supply Systems: A critical infrastructure characterized by the sources of water, reservoirs and holding facilities, aqueducts and other transport systems, the filtration, cleaning and treatment systems, the pipelines, the cooling systems and other delivery mechanisms that provide for domestic and industrial applications, including systems for dealing with water runoff, waste water, and firefighting.

**"Critical Foundations: Protecting America's Infrastructures," October 1997, as found at: http://www.dtra.mil/press_resources/publications/deskbook/full_text/Other_Relevant_References/PCCIP_Report.pdf.

[19] *Ibid.,* p. B1.
[20] *Ibid.,* p 15.

Presidential Decision Directive-63. In 1998, in response to the commission's findings, President Clinton issued Presidential Decision Directive (PDD) 63, which established a strategy for better protecting critical infrastructures and for ensuring greater cooperation between the government and private sector towards that end. The directive defined critical infrastructures as "those physical and cyber-based systems essential to the minimum operations of the economy and government."[21] It also opened the possibility of expanding the number of potential infrastructures identified as critical by stating that, "they include, *but are not limited to*, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private."[22] (Emphasis added.) PDD 63 formalized the U.S. government's policies toward critical infrastructure in three particularly significant ways. First, it established high-level roles and responsibilities for the management of critical infrastructure issues by designating lead federal agencies (known as sector liaisons), which were responsible for working with private sector counterparts (known as sector coordinators). Second, it clarified the purpose of critical infrastructure protection efforts by setting the goal of preventing or mitigating any intentional or accidental events that would significantly diminish the abilities of:

- the federal government to perform essential national security missions and to ensure the general public's health and safety;
- state and local governments to maintain order and to deliver minimum essential public services;
- and, the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services.[23]

(The PDD further emphasized that "[a]ny disruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the United States."[24]) And third, the PDD highlighted the dynamic nature of critical infrastructure issues and deliberately prepared government policy for future changes. Noting that many of the most pressing challenges relating to critical infrastructure were directly related to the growing role of information technology and automated, interlinked processes, the directive emphasized that "addressing these vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security."[25]

National Plan for Information Systems Protection. In 2000, the White House released the first version of a national plan for critical infrastructure protection[26] that had been called for in PDD 63. Although the plan focused exclusively on cyber-security aspects of critical infrastructure protection, the document is interesting because it presents a slightly expanded definition of critical infrastructure. Specifically, the plan states that:

> "Critical infrastructures are those systems and assets—both physical and cyber—so vital to the Nation that their incapacity or destruction would have a debilitating impact on national security, national economic security, and/or national public health and safety."[27]

---

[21] The White House, "Presidential Decision Directive/NSC-63 – Critical Infrastructure Protection," May 22, 1998 as found at: http://www.fas.org/irp/offdocs/pdd/pdd-63.htm

[22] *Ibid*.

[23] Moteff et al., "Critical Infrastructures: What Makes an Infrastructure Critical?" p. 15.

[24] PDD 63 as found at: http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.

[25] *Ibid*.

[26] The White House, "Defending America's Cyberspace: National Plan for Information Systems Protection. Version 1.0. An Invitation to a Dialogue," (2000), as found at: http://clinton4.nara.gov/media/pdf/npisp-fullreport-000112.pdf

[27] *Ibid*., p. vii.

This is notable because it is the first instance in which a formal policy definition of critical infrastructure has identified public health and safety as "critical" government functions to be safeguarded.

Executive Order 13228. A further expansion of the government's CI definition appeared shortly after the 9/11 attacks, when President Bush signed Executive Order 13228 – Establishing the Office of Homeland Security and the Homeland Security Council. As a sign of the reinvigorated importance critical infrastructure issues were being given in the aftermath of September 11, the new White House office was charged with "coordinate[ing] efforts to protect the United States and its critical infrastructure from the consequences of terrorist attacks."[28] While EO 13228 did not specifically define critical infrastructure, it did identify a number of infrastructure sectors requiring particular attention. (See Box 1.2.) Interestingly, the executive order included agriculture and livestock among these. This is the first time food infrastructure appears prominently in government policies concerning CI.

Box 1.2***

CRITICAL INFRASTRUCTURE DEFINITIONS FROM EXECUTIVE ORDER 13228

…The Office shall coordinate efforts to protect the United States and its critical infrastructure from the consequences of terrorist attacks. In performing this function, the Office shall work with Federal, State, and local agencies, and private entities, as appropriate, to:

…strengthen measures for protecting energy production, transmission, and distribution services and critical facilities; other utilities; telecommunications; facilities that produce, use, store, or dispose of nuclear material; and other critical infrastructure services and critical facilities within the United States from terrorist attack;

…coordinate efforts to protect critical public and privately owned information systems within the United States from terrorist attack;

…coordinate efforts to protect transportation systems within the United States, including railways, highways, shipping, ports and waterways, and airports and civilian aircraft, from terrorist attack;

…coordinate efforts to protect United States livestock, agriculture, and systems for the provision of water and food for human use and consumption from terrorist attack; …

***Executive Order 13228 – Establishing the Office of Homeland Security and the Homeland Security Council, October 8, 2001, as found at: http://www.whitehouse.gov/news/releases/2001/10/20011008-2.html.

Executive Order 13231. Little more than a week after creating the Office of Homeland Security and Homeland Security Council, President Bush signed Executive Order 13231 – Critical Infrastructure Protection in the Information Age, which established the President's Critical Infrastructure Protection Board.[29] Despite the board's expansive title, the purpose of the new entity was limited to the coordination of the "cyber-related federal efforts and programs associated with protecting"[30] critical information infrastructure systems. Although this mandate included authorization for the board to coordinate the protection of physical assets directly related to information systems, it did *not* provide the board with any authority to address other non-cyber-specific critical infrastructure matters. The introductory text of EO 13231, at least, did emphasize that the protection of such systems is "essential to the telecommunications, energy, financial services, manufacturing, water,

[28] Executive Order 13228 – Establishing the Office of Homeland Security and the Homeland Security Council, October 8, 2001, as found at: http://www.whitehouse.gov/news/releases/2001/10/20011008-2.html.
[29] The White House, "Executive Order 13231 – Critical Infrastructure Protection in the Information Age," October 16, 2001, as found at: http://www.fas.org/irp/offdocs/eo/eo-13231.htm.
[30] GAO, "Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors," p. 15.

transportation, healthcare and emergency services sectors."[31] The language in EO 13231 is indicative of two interesting trends in the government's handling of CI issues. First, the text demonstrates an ongoing "fluidity" in the way in which government uses the term "critical infrastructure." Clearly, many critical infrastructure security matters are directly related to cyber threats. By conflating cyber issues with other broader critical infrastructure issues, however, the government may be unintentionally limiting public awareness of the very serious physical CI threats that exist. Second, in the executive order's single reference to the other infrastructure sectors that are supported by information systems, it is notable that "manufacturing" is present. This, again, demonstrates a gradual expansion of the officially recognized critical infrastructures within government policy.

Critical Infrastructures Protection Act of 2001. On October 25, 2001, Congress passed the USA PATRIOT Act. Section 1016 of the Act, known as the Critical Infrastructures Protection Act, specifically defines critical infrastructures as:

> "…systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[32]

Although the legislation does not comprehensively identify the discrete infrastructures that fall into this category, it does note that "telecommunications, energy, financial services, water and transportation sectors" are examples of the types of modern interdependent systems that are essential to the maintenance of "national defense, continuity of government, economic prosperity, and quality of life in the United States."[33] Perhaps more importantly, the Act clearly articulates the U.S. government's policy regarding critical infrastructure. (See Box 1.3). Specifically, it highlights the government's commitment to minimizing the interruption of CI services, cooperating with private and public sector partners to achieve its objectives, and ensure the continuity of government (CoG) functions in all circumstances.[34]

Box 1.3****

STATEMENT OF POLICY FROM THE CRITICAL INFRASTRUCTURE PROTECTION ACT OF 2001

(c) POLICY OF THE UNITED STATES- It is the policy of the United States –

(1) that any physical or virtual disruption of the operation of the critical infrastructures of the United States be rare, brief, geographically limited in effect, manageable, and minimally detrimental to the economy, human and government services, and national security of the United States;

(2) that actions necessary to achieve the policy stated in paragraph (1) be carried out in a public-private partnership involving corporate and non-governmental organizations; and

(3) to have in place a comprehensive and effective program to ensure the continuity of essential Federal Government functions under all circumstances.

****H.R. 3162-130 (P.L. 107-56), Section 1016, as found at: http://www.epic.org/privacy/terrorism/hr3162.html.

[31] The White House, "Executive Order 13231 – Critical Infrastructure Protection in the Information Age," October 16, 2001, as found at: http://www.fas.org/irp/offdocs/eo/eo-13231.htm.

[32] H.R. 3162-130 (P.L. 107-56), Section 1016, as found at: http://www.epic.org/privacy/terrorism/hr3162.html.

[33] *Ibid*., Sec. 1016 (b) 2-3.

[34] *Ibid*., Sec. 1016 (c) 1-3.

A public White House document outlining the administration's official position on the legislation described critical infrastructures in slightly different terms, noting that they are "those assets, systems, and functions vital to our national security, governance, public health and safety, economy, and national morale." The document more specifically indicated that the administration considered the nation's infrastructures to include: food, water, agriculture, health and emergency services, energy (electrical, nuclear, gas and oil, dams), transportation (air, road, rail, port, waterways), information and telecommunications, banking and finance, energy, chemical, defense industry, postal and shipping, and national monuments and icons.[35] Although this list was not included in the final USA PATRIOT Act legislation, it demonstrates that at least some elements of the government were further expanding the concept of CI to include physical structures (such as national monuments and icons) which, if struck, could affect national morale.

National Strategy on Homeland Security. Issued by the White House in July 2002, the national strategy highlights the protection of critical infrastructures as one of six "critical" homeland security mission areas. It uses the USA PATRIOT Act's definition of critical infrastructure to frame discussion of the topic, but it also expands on the definition by presenting a specific list of critical infrastructure sectors that includes: agriculture, food, water, public heath, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemical industry, postal and shipping.[36] Although this list does not include national monuments and icons, the strategy notes separately that:

> "In addition to our critical infrastructure, our country must also protect a number of key assets – individual targets whose destruction would not endanger vital systems, but could create local disaster or profoundly damage our Nation's morale or confidence. Key assets include symbols or historical attractions, such as prominent national, state, or local monuments and icons. In some cases, these include quasi-public symbol that are identified strongly with the United States as a Nation, and fall completely under the jurisdiction of state and local officials or even private foundations. Key assets also include individual or localized facilities that deserve special protection because of their destructive potential or their value to the local community."[37]

Besides adding the concept of "key assets" to the nation's critical infrastructure policy, the 2002 strategy clarifies how the "criticality" of an infrastructure's component parts should be considered. It recognizes that "the assets, function, and systems within each critical infrastructure sector are not equally important," and that local communities will consider some infrastructures critical (local schools and courthouses, for example) which the state or federal government might not. Given this situation, the 2002 strategy calls for the development of a "consistent methodology" and funding mechanisms that will allow communities at all levels of society to identify and protect their "critical assets, systems, and functions."[38]

National Strategy for the Physical Protection of Critical Infrastructure and Key Assets. In early 2003, the White House released "The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets."[39] The 83-

---

[35] Moteff et al., "Critical Infrastructures: What Makes and Infrastructure Critical?" p. 7.
[36] White House, "National Strategy for Homeland Security," July 16, 2002, p. 30, as found at: http://www.whitehouse.gov/homeland/book/sect3-3.pdf
[37] *Ibid*, p. 30.
[38] *Ibid*.
[39] White House, "National Strategy for the Physical Protection of Critical Infrastructures and Key Assets," February 2003, as found at: http://www.whitehouse.gov/pcipb/physical.html.

page document details the government's policy to protect critical infrastructure from physical[40] terror acts that could:

- impair the government's ability to perform essential national and homeland security missions and ensure the general public's health and safety;
- undermine state and local government capacities to maintain order and to deliver minimum essential public services;
- damage the private sector's capability to ensure the orderly functioning of the economy and the delivery of essential services; or
- undermine the public's morale and confidence in national economic and political institutions.[41]

With one minor modification,[42] the 2003 strategy categorizes the nation's critical infrastructures into the same 13 categories that were identified by the 2002 National Strategy for Homeland Security and referenced previously. In its discussion of each identified sector, the document further specifies facilities and functions that might be particularly vulnerable to terrorist attack. The strategy is careful to emphasize, however, that such examples do not represent an exhaustive list of potential terror targets.

It is worth noting that the 2003 strategy establishes three strategic critical infrastructure protection objectives. "The first is to identify and ensure the protection of the most critical assets, systems, and functions in terms of national-level public health and safety, governance, and economic and national security and public confidence…The second objective is to ensure protection of infrastructures and assets facing specific, imminent threats; and the third is to pursue collaborative measures and initiatives to ensure the protection of other potential targets that may become attractive over time."[43] The document also specifies three general classifications of threats to critical infrastructure which must be guarded against. These include: 1) *direct infrastructure effects* – cascading disruption or arrest of the functions of critical infrastructures or key assets through direct attacks on a critical node, system, or function; 2) *indirect infrastructure effects*: cascading disruption and financial consequences for government, society, and economy through public- and private-sector reactions to an attack; and 3) *exploitation of infrastructure* – exploitation of elements of a particular infrastructure to disrupt or destroy another target.[44]

Homeland Security Presidential Directive-7. The most recent development in government policy relating to critical infrastructure occurred in December 2003, when President Bush signed Homeland Security Presidential Directive (HSPD) 7 – Critical Infrastructure Identification, Prioritization, and Protection.[45] This new directive establishes mechanisms by which Federal departments and agencies are to "identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks."[46] The directive defines "critical infrastructure" using the meaning given to the term by the USA PATRIOT Act, which has already been discussed. Additionally, it uses a definition found in the Homeland Security Act of 2002 to define the term "key

---

[40] The strategy does not address cyber attacks. Cyber issues are addressed in a separate February 2003 document titled, "The National Strategy to Secure Cyberspace."

[41] *Ibid*, p. ix.

[42] The 2003 strategy broadens the "Chemical Industry" category to include "Chemical Industry and Hazardous Materials."

[43] National Strategy for the Physical Protection of Critical Infrastructures and Key Assets," p.20.

[44] *Ibid*, p. viii.

[45] White House, "Homeland Security Presidential Directive 7 – Critical Infrastructure Identification, Prioritization, and Protection," December 17, 2003, as found at: http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html.

[46] *Ibid*.

resources" as "publicly or privately controlled resources essential to the minimal operations of the economy and government."[47] Unlike earlier policy statements concerning critical infrastructure, HSPD-7 links the critical infrastructure issue strongly with key resources "whose exploitation or destruction by terrorists could cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction, or could profoundly affect our national prestige and morale."[48] This focus on the potential mass damage that could come from terrorist strikes on critical infrastructures or key resources is reflected in a more detailed articulation of US policy concerning its protection efforts:

> It is the policy of the United States to enhance the protection of our Nation's critical infrastructures and key resources against terrorist acts that could:
>
> a) cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction;
>
> b) impair Federal departments and agencies' abilities to perform essential missions, or to ensure the public's health and safety;
>
> c) undermine State and local government capacities to maintain order and to deliver minimum essential public services;
>
> d) damage the private sector's capability to ensure the orderly functioning of the economy and delivery of essential services;
>
> e) have a negative effect on the economy through the cascading disruption of other critical infrastructure and key resources; or
>
> f) undermine the public's morale and confidence in our national economic and political institutions.[49]

Defining Critical Infrastructure. The preceding review of CI policy demonstrates the fluid nature and ongoing evolution of the concept "critical infrastructure." As yet, there is no definitive, widely accepted definition of the term. As PPD-63 points out, however, such dynamism in public consideration of the matter should come as little surprise given the novel nature of many emerging CI threats. Simply put, we are continuing to discover new aspects and realities (including vulnerabilities) of 21st century life. Indeed, it is fully appropriate that policymakers maintain a degree of flexibility when considering such issues so as to be best positioned for future possibilities. That said, several generalizations concerning the nature of critical infrastructure, especially in the context of terrorism, can be made.

First, critical infrastructures are made up of a vast and diverse set of systems and assets. Seeking to enhance understanding of critical infrastructure by identifying discrete categories of CI is desirable, but difficult, as new categories emerge with regular frequency, especially as technologies and system relationships change. This is why most current definitions list "examples" of critical infrastructure types, but emphasize that the examples are by no means exhaustive. Second, it is clear that almost all aspects of critical infrastructure can be very broadly recognized as either "physical" or "cyber" targets. As demonstrated by its issuance of two discrete national CI strategies – one concerning cyber issues and the other physical issues – the current administration has recognized this CI reality and formulated its policies accordingly. Acknowledging this distinction, and the

---

[47] Homeland Security Act of 2002 (6 U.S.C. 101(9)).
[48] HSPD-7 as found at: http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html.
[49] *Ibid*.

fact that both the characteristics and perpetrators of "cyber" and "physical" attacks often differ markedly from one another, the project team decided to focus this study on "physical" infrastructure. Moreover, open source information on cyberterrorism is, understandably, relatively sparse, and the project team preferred to utilize its resources as efficiently as possible.
Third, it is apparent that all definitions of CI are related to systems and services that are essential to the functioning of normal life. It is important to recognize, however, that what is deemed "essential" will vary depending on the level of the community concerned. Consequently, local, state, and national perceptions of CI will vary accordingly.

Based on the above discussion, and its own discussions on the topic, CNS offers the following definition of critical infrastructure, which will henceforth be used in this report:

> **Critical infrastructures are those physical systems that a community depends on to maintain its security, governance, public health and safety, economy and public confidence. The constituent parts of such systems will vary according to the community context in which they are viewed.**

C. Structure of Report

This report is structured as follows:

Chapter 1: Introduction and Definition of Critical Infrastructure
Chapter 2: Conceptual Background and Literature Extracts
Chapter 3: Historical Record and Selected Case Studies
Chapter 4: Critical Infrastructure Terrorist Incident Catalog
Chapter 5: The DECIDe Framework
Chapter 6: Further Research and Conclusion

Chapter 2 introduces readers to the difficulties surrounding any assessment involving terrorism and briefly outlines the main categories of terrorist ideology. It then introduces and defines the various factors used to develop the framework presented later in the report. Chapter 2 concludes with theoretical justification from the literature for the impact of these factors on target selection. Chapter 3 provides a brief overview of the historical record and proceeds with a selection of case studies examining the perpetrators and conduct of several important, but less well-known, attacks against critical infrastructure. Based on this historical analysis, this chapter offers some suggestions for the most likely source of future threats to critical infrastructure in the United States. CrITIC – the Critical Infrastructure Terrorism Incident Catalog – is described in Chapter 4, followed by a preliminary quantitative analysis of the data. The findings of Chapters 2, 3 and 4 are combined in the form of the DECIDe (Determinants Effecting Critical Infrastructure Decisions) Framework, which is described and detailed in Chapter 5. Chapter 6 suggests avenues for further development of the framework and summarizes project findings.

Chapter 2: CONCEPTUAL BACKGROUND AND LITERATURE EXTRACTS*

A. Conceptual and Methodological Issues

Before turning to the theoretical underpinnings and empirical record of terrorist groups that have intentionally targeted CI in the past, it is appropriate to make some introductory remarks about certain conceptual and methodological issues. In this section, CNS's general methodological approach is described, clarifying the meaning of the oft-misunderstood term "terrorism," identifying the principal categories of non-state terrorist groups, and illustrating why it is often difficult to determine whether terrorists are specifically targeting CI.

Basic Formula for Terrorist Threat Assessment

In order to assess the CI threat posed by particular types of terrorist groups, one must consider both their ideological motivations and their technical and operational capabilities. This analytic approach can be rendered as follows:

LIKELIHOOD OF THREAT = MOTIVATIONS x CAPABILTIES

Like most social science formulae, this one is too simplistic to reflect the complexities of reality, yet it does point squarely to the essential factors that must be considered in terrorist threat assessments. As noted previously, the focus of this study is almost exclusively directed toward the *motivations* of different types of terrorist groups. The question of a particular terrorist group's technical capabilities (in the narrowest sense) is not discussed at length, except insofar as these play specific roles targeting decisions.

The Distinguishing Characteristics of Terrorism

Perhaps the first desideratum should be to draw a clear analytical distinction between "terrorism" in the strict sense of the term and other types of non-state violence, a distinction that unfortunately needs to be made at the outset precisely because most definitions of terrorism – including those employed by some U.S. government agencies[50] – are imprecise if not entirely misleading.

---

* The introduction and definitions in this chapter were written by Jeffrey M. Bale, who also compiled, systematized, and analyzed the extracts, except for the sections on Perceptual Filters that were written by Gary Ackerman. The extracts themselves were painstakingly gathered by all members of the research team, reviewed by Andrew Jayne and Linda Serocki, and then standardized and formatted by Linda Serocki.

[50] Note, e.g., the definition from Title 22 of the U.S. Code, Section 2656f(d): "Terrorism means premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience." See www.cia.gov/terrorism/faqs.html. Here there is one unnecessary restriction (e.g., terrorism can be "religiously motivated" as well as "politically motivated") and two outright errors (terrorism is not always perpetrated against "noncombatant targets," and it is not only carried out by "subnational groups" or "clandestine agents" – the worst perpetrators of terrorism, historically speaking, have been states, who often openly employ their own security forces instead of "clandestine agents"), and the quintessential feature of terrorism – the carrying out of violence in order to influence a wider target audience – is wrongly qualified with "usually." See note 2 below.

Without spending too much time on contentious definitional questions, it can be said that the best way to distinguish between terrorism and other forms of violence is to recognize that most acts of violence are dyadic, i.e., they involve only two parties or protagonists, the perpetrator(s) and the victim(s):

Perpetrator → Victim

In marked contrast, bona fide acts of terrorism are triadic, i.e., they involve three parties or protagonists, the perpetrator(s), the victim(s), and a wider target audience (or audiences):

Perpetrator → Victim → Wider Target Audience(s)

In short, terrorism is violence that is consciously carried out by the perpetrator(s) in order to influence the attitudes and behavior of a wider target audience (or multiple target audiences). It is, as Brian Jenkins and others have aptly pointed out, violence for psychological effect.[51] Indeed, one of the many perverse ironies of terrorism is that, although the actual victims suffer its effects disproportionately and in the most direct and brutal manner, their importance is strictly secondary and derives principally from the fact that they have been specifically selected because they are viewed as symbolizing something larger or representing a broader category of persons. To put it another way, the most important nexus in any terrorist act is between the perpetrators and the target audience(s) they are trying to influence. It follows from this that targeted assassinations of particular individuals for purely instrumental reasons (e.g., murders of particularly effective or brutal policemen) or attacks that are solely designed to kill large numbers of people (e.g., massacres) are not, strictly speaking, acts of terrorism. They would only constitute acts of terrorism if their primary purpose was to traumatize and influence the behavior of wider target audiences. In many real-world cases, of course, attacks are carried out for both instrumental and psychological reasons, but *the latter would have to predominate in the eyes of the perpetrators* if such attacks are to be regarded, strictly speaking, as terrorism. Hence violent acts that inadvertently end up traumatizing people other than the actual victim, e.g., a series of rapes in a particular urban neighborhood, should not be characterized as acts of terrorism.

Thus terrorism is nothing more than a violent technique of manipulation, and like other techniques it can be used by *anyone*, whatever their ideological orientation or relationship to the state. It can be employed on behalf of state power or in opposition to state power, by left-wingers, right-wingers, or centrists, by the irreligious or the religious, and for an infinite variety of causes. One man's terrorist is therefore *not* another man's freedom fighter, as many claim; rather, one man's terrorist should invariably also be another man's terrorist, since regardless of the underlying cause involved – or whether one sympathizes with or deplores it – a terrorist can be identified purely by the methods he or she chooses to employ. It follows that only those organized groups that rely primarily on terrorist techniques can legitimately be described as terrorist groups.

However, for the purposes of this study, all non-state actors that have attacked CI in the past will be considered, even if they do not technically fall into the category of terrorists in this carefully delimited sense. That is because it seems obvious that, for purposes of homeland security, the U.S. government is interested in any and all

[51] The best collection and analysis of definitions of terrorism can be found in Alex P. Schmid and Albert J. Jongman, *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories and Literature* (Amsterdam: North-Holland, 1988), especially pp. 1- 38. Many of the better definitions highlighted therein emphasize the centrality of carrying out violent actions with the conscious intention of exerting a psychological impact on a wider target audience. Although this work is now out-of-date, we still regard it as the best single introduction to terrorism. The formal definition that one of the authors has used in his own classes on terrorism for several years is as follows: "Terrorism is the use or threatened use of violence, directed against victims selected for their symbolic or representative value, as a means of instilling anxiety in, transmitting one or more messages to, and thereby manipulating the attitudes and behavior of a wider target audience or audiences."

subnational groups that may end up threatening CI in this country, not simply those that can legitimately be characterized as "terrorist."

The Main Categories of Non-State Terrorist Groups

Once the meaning of the term "terrorism" has been clarified, the principal categories of non-state terrorists in recent decades need to be identified. There are five primary types of subnational terrorist groups that have had historical significance during and after the Cold War:

1. **Nationalist/separatist/irredentist (Ethno-Nationalist) groups** – groups relying heavily on terrorism that seek either to establish an independent state for the ethnic, linguistic, cultural, or national community with which they are affiliated, or (if they already have their own independent state) to unite all of the members of their community – including those that live in neighboring countries – under the aegis of such a state. The most important groups in this category have been the Armenian Secret Army for the Liberation of Armenia (ASALA), Euskadi ta Askatasuna (ETA: Basque Freedom and Fatherland), the Front de Libération Nationale de la Corse (FLNC: National Liberation Front of Corsica), the Irish Republican Army (IRA), the Palestine Liberation Organization (PLO), the Partiye Karkaran-e Kurdistan (PKK: Kurdistan Worker's Party), the Liberation Tigers of Tamil Eelam (LTTE, also known as the Tamil Tigers), and Sikh groups seeking to create an independent state of "Khalistan."

2. **Secular left-wing groups** – groups relying heavily on terrorism that seek to overthrow the capitalist system and either establish a "dictatorship of the proletariat" (Marxist-Leninists) or, much more rarely, a decentralized, non-hierarchical sociopolitical system (anarchists). The most important groups in this category have been the Fuerzas Armadas Revolucionarias de Columbia (FARC: Revolutionary Armed Forces of Columbia), Sendero Luminoso (SL: Shining Path) in Peru, various Maoist groups in Nepal, and the so-called "fighting communist organizations" in Europe, such as Action Directe (AD: Direct Action) in France, the Brigate Rosse (BR: Red Brigades) and Prima Linea (PL: Front Line) in Italy, the Rote Armee Fraktion (RAF: Red Army Faction) and Bewegung 2. Juni (June 2nd Movement) in Germany, the Cellules Combattantes Communistes (CCC: Fighting Communist Cells) in Belgium, the Grupos de Resistencia Antifascista Primero de Octubre (GRAPO: October 1st Anti-Fascist Resistance Groups) in Spain, the Epanastatikē Organōsē 17 Noemvrē (17N: November 17th Revolutionary Organization) in Greece, and Devrimci-Sol (DEV-SOL: Revolutionary Left) and other groups in Turkey.

3. **Secular right-wing groups** – groups relying heavily on terrorism that seek to restore national greatness (radical nationalists), suppress "subversive" opponents, expel or subordinate troublesome ethnic and cultural minorities (racists), or overthrow the existing democratic and "plutocratic" capitalist systems in order to establish a revolutionary "new order" (neo-fascists). The most important groups in this broad category have been Organōsis X (the X Organization) in postwar Greece, the Organisation de l'Armée Secrète (OAS: Secret Army Organization) in French Algeria, Aginter Presse and the Exército de Libertação Português (ELP: Portuguese Liberation Army) in Portugal, Ordine Nuovo (ON: New Order) and Avanguardia Nazionale (AN: National Vanguard) in Italy, the Aktionsfront Nationaler Sozialisten (ANS: National Socialists' Action Front) and the Odfried Hepp/Walter Kexel group in West Germany, Westland New Post (WNP) in Belgium, the Grupos Antiterroristas de Liberación (GAL: Anti-Terrorist Liberation Groups) in Spain, the Bozkurtlar (Grey Wolves) paramilitary squads affiliated with the Milliyetçilik Haraket Partisi (MHP: Nationalist Action Party) in Turkey, the Alianza Anticomunista Argentina (AAA: Argentine Anti-Communist Alliance or Triple A) in Argentina, the Frente Nacionalista Patria y Libertad (PyL: Fatherland and Freedom Nationalist Front) in Chile, vigilante ("death") squads

in various Central American countries, the Afrikaner Weerstandsbeweging (AWB: Afrikaner Resistance Movement) in South Africa, and the Minutemen and the Order in the U.S.[52]

4. **Religious terrorist groups** – groups relying heavily on terrorism that seek to smite the purported enemies of God and other evildoers, impose strict religious tenets or laws on society (fundamentalists), forcibly insert religion into the political sphere (i.e., those who seek to "politicize" religion, such as Christian Reconstructionists and Islamists), and/or bring about Armageddon (apocalyptic millenarian cults). This type of terrorism comes in five main varieties: 1) Islamist terrorism; 2) Jewish fundamentalist terrorism, primarily inside Israel; 3) Christian terrorism, which can be further subdivided into fundamentalist terrorism of an Orthodox (mainly in Russia), Catholic, or Protestant stamp (which, in the U.S., is especially aimed at stopping the provision of abortions) and terrorism inspired by the idiosyncratic Christian Identity doctrine; 4) Hindu fundamentalist/nationalist terrorism; and 5) terrorism carried out by apocalyptic religious cults. The most important groups in these subcategories have been Islamist groups such as al-Qa`ida (the Base or Foundation), Hizballah (Party of God) in Lebanon, al-Harakat al-Muqawama al-Islamiyya (HAMAS: Islamic Resistance Movement) and al-Jihad al-Islami (Islamic Jihad, also known as PIJ) in the Palestinian occupied territories, al-Tanzim al-Jihad (Jihad Organization, also known as EIJ) and al-Jama`a al-Islamiyya (Islamic Group) in Egypt, al-Takfir wa al-Hijra (Excommunication and Migration) in North Africa, the Groupe Islamique Armée (GIA: Armed Islamic Group) and Groupe Salafiste pour la Prédication et le Combat (GSPC: Salafist Group for Preaching and Fighting) in Algeria, al-Hizb al-Tahrir al-Islami (HT: Islamic Liberation Party) in Central Asia and elsewhere, Jemaah Islamiyah (JI: Islamic Community) in island Southeast Asia, the Abu Sayyaf Group (ASG) in the Philippines, and various organizations operating in Kashmir; Teror Neged Teror (TNT: Terror Against Terror) in Israel; the Phineas Priesthood, and the Covenant, the Sword, and the Arm of the Lord (CSA) in the U.S.; elements from Bajrang Dal (BD: Mighty Hanuman's Army), the youth wing of the extremist Vishva Hindu Parishad (VHP: World Hindu Council) in India; and Aum Shinrikyo (Aum Supreme Truth) in Japan.

5. **Single-issue groups** – groups relying heavily on terrorism that obsessively focus on very specific or relatively narrowly-defined causes of various sorts. This category includes organizations from all sides of the political spectrum, e.g., animal rights groups such as the Animal Liberation Front (ALF), anti-communist groups such as the Cuban exile organization Omega 7, the Comando de Caça aos Comunistas (CCC: Communists-Hunting Commando) in Brazil, or the [Grupos] Autodefensas Unidas de Colombia (AUC: United Self-Defense Groups of Colombia), and anti-abortion groups such as the Army of God (AOG) in the United States.

Needless to say, groups from each of these five broad categories have distinct ideologies that help to explain what they are for and against, who their friends and enemies are, and – most importantly for this study – what targets they believe they can legitimately attack, but it is also the case that even superficially similar groups within each of these categories and subcategories have their own distinctive doctrines. Moreover, it should be emphasized that these major categories of terrorism are not entirely discrete. Some essentially ethno-nationalist terrorist groups have had a Marxist gloss (the PKK, factions of ETA), a religious gloss (certain Sikh groups), or a combination of the two (factions of the IRA). In more recent times, essentially religious terrorist groups have also displayed acute nationalist sentiments (the Islamist groups HAMAS and Islamic Jihad in the Palestinian occupied territories), and essentially nationalist terrorist groups have adopted an increasingly prominent

[52] For an overview of postwar right-wing terrorism, which has generally been neglected (especially in Cold War Europe), see Jeffrey M. Bale, "Terrorism, Right-Wing," in Bernard A. Cook, ed., *Europe since 1945: An Encyclopedia* (New York: Garland, 2001).

religious coloration (important pro-Islamist factions within the Chechen separatist movement, such as that of Shamil Basayev).[53] These types of complexities need to be kept in mind when considering their motivations.

B. Materials Examined and Sources Utilized

In this preliminary effort to elucidate terrorist motivations for attacking critical infrastructure (CI), one of the strategies adopted by the CNS team was to review the existing scholarly literature on terrorism. Our goals for the effort were both 1) to learn whether particular authors had developed especially useful insights into this question, and 2) to discover whether any general consensus had already been reached about this subject. The review confirmed initial expectations that little to no existing literature focuses specifically on the reasons why terrorists attack infrastructural targets. Surprisingly, there was also a paucity of material regarding the more general process of target selection by terrorist groups. While this discovery enabled our research to be conducted without the preexisting assumptions that sometimes encumber terrorism research, it also meant that much of the literature reviewed was of value more for framing than directly informing the issues at the heart of our study.

More than 120 readings on terrorism and threat assessment were examined by team members in order to obtain as much relevant information as possible that might be useful in the creation of our CI terrorist attack framework. The materials consulted for this project were reasonably diverse, including government reports, unpublished conference presentations, articles found on websites but not yet published in hard copy format, and a wide range of scholarly books and articles. Most of these sources were produced by recognized experts in the fields of terrorism studies or threat assessment. It should be noted, however, that hundreds of focused empirical studies on individual terrorist groups or operations were not included in the corpus of materials, due to time limitations. As a result, our focus throughout was on the general literature on terrorism, as opposed to case studies, as well as on the threat assessment literature that may be relevant to the question of terrorist target selection. The complete list of the materials which were utilized for this phase of the process is included in the bibliography.

C. Categorization and Definitions of Factors Involved in Target Selection

Before proceeding to summarize the results of the scholarly literature dealing with target selection by terrorists, it is first necessary to identify and briefly define the factors and subfactors we considered significant enough to focus on and ultimately utilize in our model. The purpose here is not to claim that these are the only important factors, or insist that this is the only way these factors can be categorized, or provide elaborate definitions of these factors, but simply to highlight those factors that were considered important by other scholars and that we ourselves could accept as being legitimate. As a result, the main factors selected numbered twelve in all, eight of

---

[53] The mixed religious and nationalist motivations of HAMAS and Islamic Jihad are widely recognized, but it is the former that clearly predominates in these two groups (in contradistinction to the motives of their political rivals in the PLO). For the "conversion" of certain key Chechen separatist factions to Islamism and their increasing resort to terrorism, see Jeffrey M. Bale, "The Chechen Resistance and Radiological Terrorism," unpublished report, July 2003. This particular piece, which was originally prepared for the Defense Threat Reduction Agency, is presently slated for inclusion in a forthcoming CNS publication on the threat of radiological terrorism in Russia. By "Islamism" the author is referring to a radically anti-Western Islamic *political ideology* with both revolutionary and restorationist elements. The principal ideological characteristics of Islamism in all of its forms are an outright rejection of Western secular values, an intransigent resistance to Western political, economic, social, and cultural influence over the Muslim world, an extreme hostility towards less committed and militant Muslims (who are often denounced as "apostates"), and an affirmation of the importance of creating an Islamic state governed by a rigid, puritanical application of the *shari`a*. For more on Islamist doctrine(s), see Jeffrey M. Bale, "Islamism," in Richard F. Pilch and Raymond Zilinskas, eds., *Encyclopedia of Bioterrorism Defense* (New York: Wiley, 2004), forthcoming.

which fall under the rubric of "Group Characteristics" and four under the rubric of "External Factors." Subsumed under most of these general factor categories are also several subfactors.

Factors Related to the Nature of the Group

The following are the main factors related to the nature of the group that were considered:

Ideology:

Ideology refers to the basic set of political, social, cultural, and/or religious beliefs that members of the group hold. In the most rudimentary sense, it indicates what members of the group are "for" and what they are "against." Under this category we have included a number of subfactors, beginning with *World View*, which is more or less equivalent to the term "ideology" itself but can refer either to more general attitudes and orientations or, as it does here, more narrowly to the substantive contents of the doctrines espoused by members of the group. Another subfactor is *Group Norms*, which refers to the almost unconscious set of values and behavioral precepts that individuals absorb in the course of the process of socialization, both those characteristic of their general national and cultural milieus and those associated with the extremist groups to which they belong (which ironically often reflect *and* self-consciously repudiate elements of the former). Finally, there is the *Grand Strategy* of the group, which refers not so much to its underlying doctrines as to its conscious adoption of particular political, social, or religious goals and objectives, i.e., what exactly does it aim to accomplish and how does it intend to accomplish it.

Organizational Structure:

Organizational Structure refers essentially to the formal organization of the group. Just how is the group organized on paper? What exactly would it look like if one prepared a graphic diagram of its structure? Within this category there are also several subfactors, beginning with *Group Size*, which is more or less self-explanatory. Another is *Degree of Centralization*, which refers to the extent to which the various subdivisions of the organization are structurally tied to and controlled by the central "core" leadership. Related to this is its *Mechanisms of Control*, which has to do with the means by which those leader(s) ensure that their subordinates follow the instructions of their superiors within the organization. Finally, there is *Bureaucratic Sophistication*, which has to do with the organization's degree of functional specialization at various levels. In short, all of the factors that concern the formal organization of the group fall within this category.

Organizational Dynamics:

Organizational Dynamics refers to all those characteristics of the organization that are *not* embodied or reflected in its formal organizational structure and which act, behind the scenes, to facilitate or interfere with its actual functioning. Among the subfactors within this category is *Leadership Style*, which refers to the personal characteristics of the leader(s) that directly influence the manner in which he actually exercises control, such as his degrees of charisma, formality, willingness to delegate, or authoritarianism. Another is *Social Isolation*, the degree to which the group's members (including its leader[s]) are cut off from or integrated into the larger society. One possible indicator of this is the extent to which group members are forced to live clandestinely. Finally, there is *Factionalization*, the extent to which competing centrifugal and centripetal pressures affect the stability of, and the exercise of authority within, the organization. Extremist groups, unlike established bureaucratic organizations, tend to undergo a kaleidoscopic process of fission and fusion that results in considerable organizational instability, frequent schisms, and the periodic establishment of entirely new groups by breakaway factions.

Organizational Lifecycle Status:

Organizational Lifecycle Status refers to the current stage in the overall history of the group. To be more precise, it has to do with the longevity of the organization, the changes the organization has undergone over time, what its condition currently is relative to its general pattern of historical evolution, and whether it still seems to be vigorous or is instead entering into a temporary or permanent phase of decline. There are no subfactors within this category.

Demographics:

Demographics refers to the collective characteristics of the group's membership in various spheres. It includes several subfactors, most of which are self-explanatory, including *Age*, *Gender*, (level of) *Education*, and *Socio-Economic Status*, as well as several that require more clarification. Among these is *Family*, which refers to the nature of group members' family relationships, e.g., do many come from broken homes? Another is *Symptoms of Psychosis*, which refers to indicators of the percentage of group members with serious psychological problems. Still another is *Criminal History*, which refers to how many group members previously were known to be involved in criminal activities. Finally, there is *Substance Abuse*, which has to do with the proportion of members with serious drinking or drug problems, either in the past or present. Unfortunately, it is often difficult to discern key demographic characteristics of particular terrorist groups without access to inside information.

Resources:

Resources refers to the extent and diversity of the assets available to a terrorist group, since such assets are required to enable it to sustain itself over time and permit it to organize and carry out attacks. These resources fall into several categories, all of which are designated here as subfactors. They include *Financial* resources, which refers to the amount of money that the group has access to, in both the long and the short terms, so that it can effectively subsidize itself and its operations; *Logistical* resources, which refers to the support infrastructure that the group has created (e.g., to provide false documents or establish safehouses) so that its key members can function as full-time terrorists, living in clandestinity (which generally means that they cannot engage in gainful employment), and carrying out desired operations; *Physical* resources, which refers to all of the actual goods and pieces of equipment the group needs to accomplish its operational objectives, such as weapons, explosives, vehicles, communications equipment, etc.; and *Human Resources*, which refers to those persons who are not members of the group or an allied group (since this is dealt with under *Demographics* and *Other Criminal and Extremist Groups*) who, either wittingly or unwittingly are available to assist the group in various capacities. An example of a human resource would be a doctor who treats wounded group members, perhaps without being aware of the nature of their activities.

Operational Capabilities:

Operational Capabilities refers, in the most general sense, to a terrorist group's ability to plan, organize, and carry out attacks. Obviously, groups lacking such capabilities will generally find it difficult or impossible to mount successful attacks. In this context, several subfactors can be identified, some of which can be characterized as generally applicable and some of which can be viewed in part as target-specific. In the former category one can include the group members' possession of *Specialized Skills* (of a non-technical sort); their degree of *Technical Expertise*, which allows them to devise and/or manufacture sophisticated weapons and equipment as needed; their *Propensity to Innovate*, which refers to their willingness to employ novel weapons and attack modalities; their *Networking Abilities*, which can either serve to facilitate or hinder their forging of useful

alliances and contacts; and their *Familiarity with the Target Environment*, which refers to their ability to blend into the regional, national, social, ethnic, or cultural milieus in which they are hoping or planning to launch attacks. More specific to particular targets is the group members' *Knowledge of the Target*, which refers to their familiarity with the type of target (for instance a group member familiar with the operation of water processing plants in general), or even with aspects of a particular target, such as the area surrounding the target, the layout of the target itself, the security measures in place there, potential infiltration and exfiltration routes, who resides nearby, where local police stations are in relation to the target, etc.

Factors External to the Group

The following are the main factors outside the group that were considered:

Historical Context, Events, and Precedents:

Historical Context refers both to the general historical milieu within which the group is operating and carrying out its actions and to various subfactors specific to that context, all of which serve to condition its decision-making processes and thereby impact upon its operational activities. Among those subfactors are *Pre-Existing Ideas*, the ensemble of values, norms, ideas, ideologies, and doctrines characteristic of that historical and cultural context which consciously or unconsciously affect the attitudes of members of the group. Few indeed are the extremist and terrorist groups whose ideas are created sui generis, without any reference to prior intellectual traditions or ingrained local attitudes. Another subfactor involved has to do with the *Symbolic Events* viewed as significant in that particular historical context, whether by the majority of people within it, members of the terrorist group itself, or both. To the extent that the symbolic importance of those events is recognized and felt by both the terrorists and members of the wider society, the former are better able to exploit them propagandistically and perhaps obtain more popular support. Symbolic events can have occurred at any point in time, from the distant past, to the recent present, in the latter case potentially acting as "trigger" events. Still another subfactor is the group's *Existing Modus Operandi*, which (to the extent that it has met with success in the past) is bound to influence the modalities of its future attacks. Finally, *Past Operational Successes and Failures*, whether those involving itself or other terrorist organizations, are likely to exert an influence on every terrorist group's future planning. Prior successes and failures serve as useful examples, whether positive or negative, and thereby provide valuable lessons that terrorist groups must learn if they wish to be successful.

Relations with External Actors:

Relations with External Actors refers to all of the parties (e.g., constituencies, organized groups, and institutions) outside the terrorist group whose reactions must be taken into consideration or with which it must successfully interact in order to achieve its objectives. These parties have been divided into several types, all of which are therefore identified as subfactors, including the group's own *Sympathizers*, who the terrorists cannot afford to alienate with their actions. Two other parties whose reactions the group must consider are the *Non-Targeted Public*, members of the populace who are not specifically targeted but who the group hopes to influence and not alienate entirely by its actions, and the *Targeted Public*, members of which are viewed as "enemies" that the group's actions are specifically meant to exert a psychological impact upon. Other external actors include the *Mass Media*, whose coverage the group hopes to exploit in order to publicize its cause, transmit messages to target audiences, rally its supporters, and frighten its enemies; *Other Extremist and Criminal Groups*, which the group may seek to establish collaborative relationships with or, if they are rivals, overshadow by means of its own successes; and elements within the *State Apparatus* which it is covertly colluding with, seeking to co-opt, or actively targeting. Terrorist groups do not operate in a vacuum and must therefore always take external forces into consideration, especially given that their acts of violence are, by definition, specifically intended to manipulate external attitudes and/or behavior.

Security Environment:

Security Environment refers to the entire array of security forces, measures, and arrangements with which the terrorist group must cope in order to operate and carry out its objectives. Unless they can successfully circumvent or surmount existing security arrangements, generally by relying heavily upon the element of surprise, terrorists cannot hope to accomplish their goals. There are no subfactors within this category.

Critical Infrastructure Characteristics:

Critical Infrastructure Characteristics refers, as the phrase itself suggests, to the distinctive features of various infrastructural targets that a terrorist group might choose to attack. The subfactors within this category include *Physical Features*, which refers to such things as the size of the facility, the layout of the site, and the level of protection on-site, etc.; *Geographical Location*, which refers to where the facility is located in relation to population centers, other strategic locales such as ports, major roadways, bridges, and airports, and the terrorist group's own operational bases; and *Function*, which refers to what type of infrastructure it is (e.g., a chemical plant, an oil pipeline, a dam) and, by extension, what effect destroying it would be likely to have on the country's ability to function normally (i.e., would it disrupt regional power temporarily, destroy an entire section of the nation's energy industry for a long time, seriously interfere with the functioning of the government, and/or produce massive civilian casualties?).

Decision-Making Factors

Before actually turning to the factors that fall under this rubric, a few preliminary remarks need to be made. To begin with, by definition terrorism is a form of purposive, directed violence, as opposed to unreflective, random violence. Terrorist target selection is thus intimately related to the specific effects that particular terrorists are seeking to generate, either as a result of or in response to their actions. Indeed, far from employing violence senselessly or pointlessly, terrorists are normally acutely aware of the overall effects they hope to produce by carrying out specific attacks.[54] It follows that if analysts can determine what it is that a terrorist group is aiming to achieve through the use of violence, they will be better able to identify and delimit the range of potential targets that that group is likely to consider attacking.[55]

Next, a few words should be said concerning nomenclature. Several scholars, including Drake who has written most extensively on the topic, view terrorist strategy as something that flows from ideology and then leads eventually to target selection. However, Drake employs the term "strategy" in a very restricted sense, specifically as "an assessment of the reactions which the terrorists wish to evoke in certain psychological targets in order to promote their political objectives."[56] This particular formulation presents at least two distinct difficulties. First, while most good definitions of terrorism emphasize that it applies to acts of violence that are intended to influence the perceptions and behavior of an audience that is far wider than the pool of actual victims, and it is true that terrorists typically select their victims so as to cause a desired psychological reaction in a much broader audience,[57] there are many cases in which members of terrorist groups have conducted attacks for reasons that have little or nothing to do with transmitting messages to others or engaging in psychological intimidation. This includes, for example, revenge killings and instrumental attacks on military facilities or personnel. One can of course technically exclude such attacks from the category of terrorism, or simply view them as non-terrorist actions perpetrated by terrorists.

---

[54] Drake, pp. 38-9.
[55] *Ibid*, p. 177.
[56] *Ibid*, p. 177.
[57] *Ibid*, p. 181.

Yet this approach is singularly unhelpful for the purposes of a threat assessment which seeks to prepare our country for any and all attacks by groups popularly viewed as terrorists, irrespective of their subjective intentions for launching those attacks. The second difficulty arises from the fact that in the case of terrorism, the line between strategy and tactics is somewhat blurred – terrorists, unlike military commanders, do not necessarily make a clear distinction between the two.[58] Indeed, Brian Jenkins has observed that "many terrorist groups fail to progress from the tactical concerns of planning specific operations to devising a strategy to achieve their political objectives."[59] These two problems could be obviated by redefining the term "strategy" in connection with terrorism, but as will become clear below we have instead chosen to use a less ambiguous term – "operational objectives."

In any case, the following were selected as the main factors involved in the decision-making process of terrorists:

General Planning Characteristics:

General Planning Characteristics refers to the decision-making mechanisms and processes of terrorist organizations in the broadest sense of those terms, as opposed to their lower-level operational objectives and their specific attack modalities. There are two subfactors within this category. One is *Decision-Maker Time Horizon*, which refers to the group's perception of how much time its members believe they have before they must carry out a projected action. This factor may be affected by both objective developments, such as changes in the security environment, or subjective notions, such as a perceived doctrinal need to carry out an attack on the anniversary of some event, real or sacred, that the group considers particularly significant. The second is *Risk Threshold*, which refers to the levels of risk the group is willing to take in order to achieve its objectives. For example, would it risk carrying out a spectacular attack even though the probability of success was lower and the safety of its members less certain, or opt to carry out a lower-level attack with a higher likelihood of success? Is it more prone to keep using conventional terrorist weapons or to innovate and shift to more unconventional but destructive weapons, even though acquiring or employing these latter might well precipitate much higher levels of state repression? In short, is a particular group bold or cautious when choosing its weapons and selecting its targets?

Perceptual Filter:

Although the literature surveyed does not deal explicitly with perception in the context of target selection, there is a significant body of work that discusses how information is 'framed' (often unconsciously) by the perceptual filters of information collectors, disseminators and users in political-military organizations. These filters reflect cognitive and affect-based biases that exclude, distort and attach idiosyncratic meaning to incoming information and can shape decisions to varying degrees.

---

[58] Mark Juergensmeyer questions the wisdom of using terms such as "strategy" and "tactics" to refer to the symbolic operations carried out by certain types of terrorist groups. According to him, the term strategy "implies a degree of calculation and an expectation of accomplishing a clear objective that does not jibe with such dramatic displays of power as the World Trade Center bombing." Similarly, he argues that these types of actions are not tactics "directed toward an immediate, earthly, or strategic goal." See *Terror in the Mind of God: The Global Rise of Religious Violence* (Berkeley: University of California, 2000), p. 123. Juergensmeyer's observation seems applicable to the World Trade Center bombing, the Oklahoma City bombing, and the 1998 bombings of the U.S. embassies in Africa.

[59] Brian M. Jenkins, *Soldiers versus Gunmen: The Challenge of Urban Guerrilla Warfare* (Santa Monica: RAND, 1974), p. 4.

Operational Objectives:

Operational Objectives refers to all of those results that terrorists seek to achieve by carrying out a particular attack, both in the short term and in the longer term. It is somewhat akin to the term "strategy" in normal military parlance, but as noted above that term can be quite misleading in regard to terrorism. Moreover, most of the comments in the literature that refer to strategy are equally applicable to the term operational objectives, which in our context has a somewhat broader connotation than strategy,[60] whereas the reverse is not necessarily true. Finally, it should be emphasized that, in contradistinction to ideology, which is relatively stable in at least the short and medium terms, the operational objectives of an attack constitutes a dynamic variable that can fluctuate dramatically according to circumstances that are both internal and external to the terrorist group.

Attack Modalities:

Attack Modalities refers to the actual methods and techniques that terrorists choose to employ to attack particular targets. There are several subfactors in this category, including *Choice of Weapons*, which is self-explanatory, and *Choice of Tactical Methods*, which refers to the actual mechanics used to approach the target, carry out the attack, and withdraw after the attack is carried out. Another is *Insiders and Outsiders*, which refers to whether the terrorist group has infiltrated its own personnel into the facility's workforce or managed to co-opt someone who already works there, i.e., has assistance from an insider. For understandable reasons, attacks that are launched with inside help may well have a better chance of success. Depending upon the choice of targets, the potential array of attack modalities can be quite extensive and diverse.

Target Selection:

Target Selection refers to the process by which terrorists first identify and later choose targets to attack. As experienced terrorism researchers know, different groups make decisions somewhat differently, if not in an entirely idiosyncratic manner. That said, this process of selection is normally involves several general stages. First, there is typically a preliminary planning phase in which more than one potential target is considered for attack. Second, those targets are all examined and evaluated, if possible via direct reconnaissance on the ground. If they still seem promising, they may be brought under more regular but discreet surveillance. Less promising targets are progressively weeded out and discarded, leaving only one (or a handful) to be decided upon. In the end, the actual targets are selected on the basis of their perceived importance, vulnerability, and suitability for accomplishing the group's aims.

These, then, are the factors and subfactors that have been employed, both in our analysis of the literature and in our model.

D. Literature Extracts Related to Target Selection for Each Factor

It is now time to examine what can be gleaned from the existing scholarly literature about each of the factors identified above as being potentially significant in terrorist target selection. The format adopted below will be to present the most valuable ideas from the literature about how these factors might influence target selection in a series of bullet points. Those points will then be followed by a summation and brief analysis. Once again, the factors will be divided into three broad categories: Factors Related to the Nature of the Group, Factors External to the Group, and Decision-Making Factors.

[60] Where the use of the term strategy is not applicable to the discussion of operational objectives, this will be noted.

However, a few words should first be said about the nature of the evidence proffered by the sources that have been consulted. Most of the claims concerning the various factors in this literature sample turned out to be based on a combination of self-evident realities, the opinions of other experts, and a few illustrative examples. The authors' general conclusions were rarely if ever derived – at least explicitly – from a careful in-depth qualitative study of specific terrorist groups, much less from a systematic comparison between such groups. Large-sample quantitative studies of any type were almost completely absent. Only a few authors with an interest in game theory carried out any type of modeling, and in that handful of cases there is little evidence of their close familiarity with "really-existing" terrorist groups. In short, most of the analyses of the factors and subfactors found herein can best be described as impressionistic or overly abstract. On the other hand, their observations generally conform to the existing scholarly consensus, sometimes contain useful insights into particular issues, and are rarely at variance with the actual behavior of terrorist groups as revealed by the historical record.

Factors Related to the Nature of the Group

1) Ideology:

In this section it is useful to divide scholarly assessments into two categories: 1) general conclusions about the role played by ideology in target selection; and 2) those that are specific to particular types of terrorist groups. In the general category, the following points are emphasized:

- "Ideology provides a motive – and possibly a formula – for action."[61]
- "The touchstone for a group's initial decisions about target selection is provided by the group's ideology."[62] This is because the ideology of a terrorist group "identifies the 'enemies' of the group by providing a measure against which to assess the 'goodness' or 'badness', 'innocence' or 'guilt' of people and institutions."[63]
- Terrorists' "tactical and targeting choices correspond to, and are determined by, their respective ideologies, attendant mechanisms of legitimization and justification and, perhaps most critically, by their relationship with the intended audience of their violent acts."[64]
- "The tactics and targets of various terrorist movements, as well as the weapons they favour, are therefore ineluctably shaped by a group's ideology, its internal organizational dynamics, the personalities of its key members and a variety of internal and external stimuli." The "target audience' at whom the act is directed" is among the main factors taken into account.[65]
- "Whilst the ideology of the terrorist group is not the sole determinant of its target selection, it is important because it…helps to form their views as to who or what may be seen as a legitimate target. By establishing such parameters, ideology is influential in determining their initial range of potential targets."[66] However, "this concept of 'legitimacy' is seen in terms of the group's beliefs and may often be far removed from what is seen as legitimate or moral behavior" by others.[67]
- Most terrorists seem to operate under "self-imposed moral and practical restraints," which means that they only see certain targets as legitimate.[68]

---

[61] Drake, *Terrorists' Target Selection*, p. 16.
[62] *Ibid*, p. 175.
[63] *Ibid*, pp. 23-24.
[64] Bruce Hoffman, "The Modern Terrorist Mindset: Tactics, Targets, and Technologies," Columbia [University] International Affairs Online, Working Paper, October 1997, p. 1.
[65] *Ibid*, p. 1. Also important, albeit less so, are the target audiences *on behalf of whose interests* the terrorists claim to carrying out their attacks.
[66] Drake, *Terrorists' Target Selection*, p. 34.
[67] *Ibid*, p. 175.
[68] *Ibid*, pp. 171-172.

- Terrorists "seek to identify their victims as being in some way 'guilty' and deserving of the treatment meted out to them. This absolves them – at least temporarily – of feelings of guilt for their actions…"[69]
- "Another important effect of ideology is that it transforms people or objects into representative symbols."[70]
- "Ideology allows terrorists to displace the blame for their actions onto other people", since the "guilt" of the physical or psychological targets is "held to make the terrorists' actions inevitable."[71]
- "Dehumanization of the intended victims…[helps to] facilitate actions by inhibiting the social and emotional factors that would typically suppress an aggressive response."[72]
- "When operations are pre-planned, a number of people or things may be selected on the basis of their ideological legitimacy as targets, with the intention of choosing one of them as the final target after other factors have been considered."[73]
- "Not all terrorist attacks are preceded by a detailed ideological inquiry. Where the target is readily identifiable, and any decisions as to the guilt of the target have been made, target selection is quite straightforward…"[74]
- "Sometimes, the ideological justification for an attack is supplied after the attack has occurred rather than having been worked out beforehand."[75] This can be done for either narrowly doctrinal or cynically instrumental purposes, e.g., on one occasion the Red Brigades devised a new explanation to cover up the fact that they had made an attack on the wrong target.
- The "philosophical and ideological views of a group – including both the espoused philosophy of the organization and the 'actual' philosophy revealed by the group's actions – are also critical in determining whether it will seek out new technology."[76]
- The groups that are most likely to pursue and successfully deploy new technologies are those that are "tapped into new technology options, open and hungry for new ideas, willing to take risks, not afraid to fail, and driven by its environment to pursue novelty…"[77]
- Group types and their associated ideologies are one of the five main variables in determining whether they will employ CBRN weapons in acts of terrorism; indeed, "weapon system selection is considerably dependent on target selection and desired outcomes because not all weapon systems will have the same effect on a given target." Hence Ehud Sprinzak's "predominant focus is on the *types* of groups most likely to be implicated in [different] scenarios…"[78]
- "In applying game theory to terrorism, it is important to leave behind popular notions of rationality, and to return to [the formal notion] that actions are taken in accordance with specific preference relations. There is no requirement that a terrorist's preference relation should involve economic advantage or financial gain…Nor is it necessary that a terrorist's preference relation conform with those of society at large."[79]

---

[69] *Ibid*, p. 25.
[70] *Ibid*, p. 25.
[71] *Ibid*, p. 28.
[72] Marisa Reddy Pynchon and Randy Borum, "Assessing Threats of Targeted Group Violence: Contributions from Social Psychology," *Behavioral Sciences and the Law* 17 (1999), p. 353.
[73] Drake, *Terrorists' Target Selection*, p. 56.
[74] *Ibid*, p. 28.
[75] *Ibid*, p. 29.
[76] Brian A. Jackson, "Technology Acquisition by Terrorist Groups: Threat Assessment Informed by Lessons from Private Sector Technology Adoption," *Studies in Conflict and Terrorism* 24 (2001), p. 193.
[77] *Ibid*, p. 203.
[78] Arpad Palfy, "Weapon System Selection and Mass-Casualty Outcomes," *Terrorism and Political Violence* 15:2 (Summer 2003), pp. 83-84.
[79] Gordon Woo, "Understanding Terrorism Risk," Risk Management Solutions report, http://www.rms.com/Publications/UnderstandTerRisk_Woo_RiskReport04.pdf , p. 8.

As for ideologies specific to certain groups, in particular religious terrorists, here are a few sample conclusions:[80]

- "The beliefs of many groups form ideological hybrids."[81]
- There may be "notable differences in targeting between groups with apparently similar ideologies…"[82]
- "It remains useful to distinguish between rationalists and expressionists: between those who employ terrorism on behalf of an external goal and those whose goal is to carry out acts of terror."[83]
- For religious terrorists, violence "still has an instrumental purpose but, unlike [for] secular terrorists, it is often an end in itself…"[84]
- All terrorists live for a future when they will assuredly triumph, but for the religious groups, "this future is divinely decreed and the terrorists themselves specifically anointed to achieve it."[85]
- "Whereas in secular terrorism, the rewards of victory are finite, in religious terrorism they are infinite: national determination, compared with paradise."[86]
- Religious terrorist attacks may not be made to achieve calculated strategic and tactical goals, but rather to serve as "dramatic events intended to impress for their symbolic significance."[87]
- "In its extreme interpretations, religion appears to be a strong driving force for the application of ruthless violence to achieve supposedly sacred objectives."[88]
- "A readiness to resort to unrestricted violence springs from a conviction that one is acting in the name and on the order of the highest, that is, divine, authority…From this, a sharp demarcation between 'us' and 'them'…"[89]
- "The strategic objectives [of religious terrorists] are long-term and potentially unlimited."[90]
- Terrorists inspired by religion are "virtually impermeable to rationalist counter-arguments", since their enemies are identified with the "forces of evil."[91]
- "Today, religious, ethnic, and national motivations and beliefs, not subject to compromise or negotiation, form the basis of an increasing number of terrorist acts against U.S. personnel, property, and interests."[92]

---

[80] Note that this is a very small and unrepresentative sample derived from the general literature CNS consulted. Every single monograph or article dealing with particular terrorist groups (or categories of groups) describes their ideological motivations and, implicitly or explicitly, how this may affect target selection.

[81] Drake, *Terrorists' Target Selection*, p. 22.

[82] *Ibid*, pp. 32-33.

[83] Gordon H. McCormick, "Terrorist Decision Making," *Annual Reviews in Political Science* 6 (2003), p. 480. This point has also been emphasized, at even greater length, by Ralph Peters, "When Devils Walk the Earth: The Mentality and Roots of Terrorism, and How to Respond," reprinted in his *Beyond Terror: Strategy in a Changing World* (Mechanicsburg, PA: Stackpole, 2002), pp. 22-65. Peters divides terrorists into "practical terrorists" and "apocalyptic terrorists," which correspond roughly to McCormick's "rationalists" and "expressionists." However, as Peters himself notes, it might be a mistake to draw a distinction that is too hard and fast between these two hypothesized categories of terrorists, since in the real world the borders between them sometimes blur.

[84] Hoffman, "Modern Terrorist Mindset," p. 7.

[85] *Ibid*, p. 8.

[86] Gavin Cameron, *Nuclear Terrorism: A Threat Assessment for the 21st Century* (New York: St. Martin's Press, 1999), p. 159.

[87] Juergensmeyer, *Terror in the Mind of God*, p. 123.

[88] Harald Muller, "Terrorism, proliferation: a European threat assessment," Institute for Security Studies, *Chaillot Papers* #58 (March 2003), p. 24.

[89] *Ibid*, p. 28.

[90] *Ibid*, p. 30.

[91] *Ibid*, pp. 28-29.

[92] United States, House of Representatives, 106th Congress, Second Session, Subcommittee on National Security, Veterans Affairs and International Relations of the Committee on Government Reform, July 26, 2000 Hearing, *Combating Terrorism: Assessing Threats, Risk Management and Establishing Priorities* (Washington, DC: Government Printing Office, 2000): http://www.gpo.gov/congress/house.

These are the principal conclusions from the literature concerning the role played by ideology in terrorist target selection.

Analysis:

There is general agreement that ideology plays a decisive role in the general process of *target selection*. By identifying clearly who the enemy ("them") is and then providing a clear explanation of why it is legitimate for members of the group ("us") to attack that enemy, ideology provides the essential rationale for a terrorist group's targeting and identifies precisely what the permissible range of targets is. However, since ideology can only provide overall guidelines concerning who (and what) *should and should not* be attacked, the selection of specific targets within that broad range of ideologically acceptable targets, including those that *can* actually be attacked, is undoubtedly based on other factors that can best be described as more narrowly strategic or tactical. That is why Drake's insistence that groups with similar ideologies can select different types of targets to attack is so important. He also goes so far as to conclude that ideology, by identifying which targets are legitimate, provides terrorist groups with both *a motive and a formula for taking action*. Moreover, by first identifying the range of potential targets and then providing a rationale for selecting them to achieve particular political objectives or psychological effects, including the transmitting of messages to one or more target audiences, ideology also indirectly affects the *choice of weapons* and *choice of tactics* to be employed, since as Palfy points out, "not all weapon systems [and, by extension, not all attack modalities] will have the same effect on a given target." Finally, by dehumanizing the enemy, ideology can also serve to *weaken normal moral constraints* that might inhibit recourse to extreme violence. At the same time, ideology also plays a role in influencing a terrorist group's *degree of technological innovation*. Together these last two factors in turn affect a group's *propensity to carry out acts of mass casualty and CBRN terrorism*.

The question of how ideologies might affect target selection cannot easily be answered in a general way, but tends to be dependent upon the specific nature of those ideologies. Moreover, some have argued that the terrorists *take action in accordance with their own internal logic or rationality*, since their doctrinal tenets and attitudes are generally at variance with those of the larger society. This means that their targets will not necessarily be chosen for the same types of pragmatic and instrumental reasons that tend to motivate others with less extreme ideologies, such as the material gain or the achievement of limited, practical objectives. According to certain authors, terrorists will often attack high-profile targets solely because of their *symbolic* value or even carry out attacks for purely *expressive* (i.e., internal psychological) reasons, rather than on the basis of ostensibly rational "cost-benefit" calculations. It may be, then, that terrorists will prove to be *impossible to dissuade or deter*, since they could be impervious to normal, rational counterarguments and/or unwilling to compromise or negotiate.

Specific Group Type Factors

The references in our readings to specific group ideologies and their effects are generally few and far between. The general consensus seems to be that, whereas nationalist/separatist and secular left-wing terrorist groups usually do not carry out acts of indiscriminate or mass casualty violence because they wish to maintain the support of their constituents, actual or proclaimed, and that secular right-wing terrorist groups also have some self-imposed limits, this is not necessarily the case with religious terrorists. Indeed, *religious terrorists often display a readiness to resort to unrestricted violence*, since they believe that their actions are carried out on behalf of, and are therefore all sanctioned by, divine authorities. Moreover, their *objectives are potentially unlimited and cosmic in their scope*, as opposed to being limited to the achievement of attainable, practical, and short-term this-worldly goals, and as a result they are probably the *least likely to dissuade and deter*. In the literature surveyed, there were no discussions of ideology that were specifically related to decisions to target CI.

2) Organizational Structure

There are only a few references in the literature to aspects of a terrorist group's organizational structure that might affect target selection:

- "The size of the group can determine the types of operation which it can carry out."[93]
- Larger organizations can "carry out more actions, including actions against less prominent targets."[94]
- "A larger terrorist group can obtain more information in relation to possible targets…"[95]
- "In the absence of confounding factors, the larger an organization, the more likely its members are to possess the appropriate explicit and tacit knowledge base to efficiently absorb new technology and the more likely it is that the organization can 'afford' to devote some of its members to technology acquisition activities."[96]
- "Good technology transfer…requires extensive face to face interactions and hands-on training…If a movement chooses to organize itself using a 'cell' or 'leaderless resistance' model – where small independent groups operate in varying degrees of ignorance about the plans and intentions [of] other group members – technology adoption by the entire movement will be essentially impossible."[97]
- In small, cell-like organizations, "the group becomes the only source of information regarding the outside world, and the sole source of security in the face of external pursuit. The group, or more likely the dominant members of the group, interprets events and ideology for the individual, determines a collective moral code, determines which targets are legitimate, and confirms the rightness of the groups' actions."[98]

Analysis:

Although none of the literature explicitly addresses the relationship between group structure (such as group size, degree of centralization, bureaucratic sophistication, and mechanisms of control) and the motivations terrorists might have for attacking CI, some scholars point to the influence that group structure can have on terrorist target selection more generally. Implicit in such discussions is the notion that group size is often correlated directly with an organization's levels of resources, capabilities, and functional specialization. Thus the literature tacitly suggests that larger groups will be both more likely to consider and more capable of effectively conducting elaborate attacks, because 1) they will generally be able to consider larger potential target sets, and 2) they will often have the wherewithal to conduct more sophisticated and resource intensive attacks. It may also be that an organization's degree of centralization may affect its ability to carry out larger-scale attacks, although the example of al-Qa`ida suggests otherwise.

[93] Drake, *Terrorists' Target Selection*, p. 80.
[94] *Ibid*, p. 34.
[95] *Ibid*, p. 79.
[96] Jackson, "Technology Acquisition by Terrorist Groups," p. 202.
[97] *Ibid*, p. 200.
[98] Drake, *Terrorists' Target Selection*, p. 168.

3) Organizational Dynamics

There are limited references in the literature to the impact of organizational dynamics on target selection:

- "…The response of any organization to external stimuli…is strongly affected by the characteristics of its leaders and how information is transmitted from the leadership to the remainder of the group…As a result, to the extent that the background and views of individual terrorist leaders can be assessed, those characteristics can be used to help predict the desire to pursue a given course of action."[99]
- Social identity theory argues that group social identity – in particular the "in-group/out-group bias" – can play a significant role in framing and biasing terrorist perceptions of targets and other external factors (such as target populations, global events, etc.).[100]
- "Groups with authoritarian/totalitarian leadership are characterized by closed decision-making bodies and processes that are restricted to the leader and personnel designated by him."[101]
- "More violent or impetuous members of a group, can force the leadership to endorse [more extreme] actions retrospectively for fear of losing the group's internal cohesion or even splitting the organization."[102]

These are the only relevant references in the literature on organizational dynamics that might affect a terrorist group's targeting.

Analysis:

The literature identifies no specific relationships between group dynamics (such as leadership style, social isolation, and factionalization) and the motivations terrorists might have for attacking critical infrastructure. Generally speaking, however, the literature does emphasize two important points. First, it notes the critical role that group leaders play – especially if they are charismatic, authoritarian, or totalitarian in nature – in establishing their organization's priorities, including its target selection preferences and priorities. Second, it suggests that if groups undergo schisms and factionalization, this may broaden the range of potential targets the various factions consider attacking and increase the pressure on rival factions to conduct more brutal and destructive attacks.

4) Organizational Lifecycle Status

The following two points have been mentioned in the literature about the role that an organization's lifecycle status might play, at least indirectly, in target selection:

- "The strategic rationale for conducting terrorist attacks typically evolves during the course of the fight…[Initial] actions designed to accelerate mobilization tend to diminish once this process is underway and the correlation of forces has begun to shift in favor of the rebels…The primary function of violence at this stage is to provoke, disorient, raise popular consciousness, and eliminate or contain the terror[ist] group's (internal and external) rivals. If all goes according to plan, the importance of these tactics can be expected to decline as the conflict takes on the characteristics of a force-on-force

[99] Jackson, "Technology Acquisition by Terrorist Groups," p. 193.
[100] Pynchon and Borum, "Assessing Threats of Targeted Group Violence," p. 345.
[101] Jerrold M. Post, Keven G. Ruby, and Eric D. Shaw, "The Radical Group in Context: An Integrated Framework for the Analysis of Group Risk for Terrorism," *Studies in Conflict and Terrorism* 25 (2002), p. 87.
[102] Drake, *Terrorists' Target Selection*, p. 80.

competition between the state and an increasingly regularized opposition."[103] In short, earlier symbolic organization-building attacks gradually give way to full-blown guerrilla or semi-conventional combat.

- "An almost Darwinian principle of natural selection also seems to affect all terrorist groups, so that every new terrorist generation learns from its predecessors, becoming smarter, tougher, and more difficult to capture or eliminate…Not only are successor generations smarter than their predecessors, but they also tend to be more ruthless and less idealistic. For some, in fact, violence becomes almost an end in itself – a cathartic release, a self-satisfying blow struck against the hated "system" – rather than being regarded as the deliberate means to a specific political end embraced by previous generations."[104]

Analysis:

There is nothing in the literature that relates a terrorist organization's lifecycle status directly to its target selection. The first point made above is somewhat problematic. Thornton himself admits that in most cases his hypothesized shift from irregular to regular warfare does not occur, mainly because most terrorist and insurgent groups never achieve sufficient levels of military power to enable them to make such a shift. Moreover, today such a transition can only be considered a possibility in a very limited number of cases, specifically those of successful Marxist (or even non-Marxist) insurgent groups that have consciously adopted certain Maoist conceptions of People's War, such as the Fuerzas Armadas Revolucionarias de Colombia (FARC: Revolutionary Armed Forces of Colombia), Sendero Luminoso (Shining Path) in Peru, and Maoist guerrillas in Nepal. On the other hand, Hoffman's point seems far more applicable in the present circumstances. Successive generations that arise within particular terrorist groups sometimes are *less idealistic and often display a greater capacity for violence*, which might well have an impact on their operational objectives and consequent target selection. Some have degenerated into criminality, such as the FARC and the Abu Sayyaf Group (ASG), whereas others have eschewed the more limited, organization-building actions of their forbearers and moved toward the planning of mass-casualty, apocalyptic-style attacks.

5) Demographics

There is no specific information in the general literature concerning the role that demographic factors play in a group's target selection process. Most of the material concerning the demographic characteristics of terrorists involves efforts to determine whether terrorists have abnormal personalities or not. While Jerrold Post has tentatively characterized certain kinds of terrorists as "marginal, isolated and inadequate individuals from troubled family backgrounds,"[105] the general consensus among scholars is that *terrorists cannot generally be considered psychologically or pathologically disturbed individuals*, at least not in any clinical sense. Indeed, terrorists exhibit a diversity of "personality traits" and have a "wide range of backgrounds,"[106] making it almost impossible to associate them with particular personality types. The most that one can say is that *terrorists tend to be profoundly alienated from mainstream values and/or institutions in their own societies*, and that younger members of terrorist groups tend to be more hotheaded and less reflective than older members, but at most such tendencies would exert an indirect effect on targeting.

---

[103] McCormick, "Terrorist Decision Making," p. 485, referring to the scheme outlined by Thomas P. Thornton, "Terror as a Weapon of Political Agitation," in Harry Eckstein, ed., *Internal War: Problems and Approaches* (New York: Free Press of Glencoe, 1964), especially pp. 82-95.

[104] Bruce Hoffman, *Terrorist Targeting: Tactics, Trends, and Potentialities* (Santa Monica: RAND, 1992), p. 5.

[105] Jerrold Post, "Notes on a Psychodynamic Theory of Terrorist Behavior," *Terrorism* 7:3 (1984), p. 241. Even Post acknowledges, however, that they are not normally mentally disturbed.

[106] McCormick, "Terrorist Decision Making," p. 494.

6) <u>Resources</u>:

This section has been divided into financial, physical, and logistical resources that correspond to the subfactors for this category:

Financial Resources

- **"**Unless they have a rich idealist funding their actions, most terrorists operate on a shoestring budget."[107]
- "Growing state sponsorship of terrorism has serious consequences. It puts more resources in the hands of the terrorists: money, sophisticated munitions, intelligence, and technical expertise. It also reduces the constraints on terrorists, permitting them to contemplate large-scale operations without worrying about alienating perceived constituents or provoking public backlash, since they need not depend on the local population for support. Without the need to finance themselves through bank robberies or ransom kidnappings and without the need to carry out operations just to maintain group cohesion, state-sponsored terrorist groups operate less frequently than groups that receive little or no state support, but they are many times more lethal and have far greater operational reach."[108]
- "Terrorist groups need money to buy weapons and their components, to rent or buy transport and accommodation, acquire or forge documents, and provide for the living expenses of their members."[109]

Physical Resources (Equipment, Weapons, Shelter, Transportation, etc.)

- "The weapons available to terrorists are very important in determining the targets which they can hope to attack successfully. The clandestine nature of terrorist operations means that smaller firearms are generally more suitable because they can be easily concealed when being moved and when approaching the target."[110]
- "When selecting their targets, terrorists' options are circumscribed by their capabilities. The weapons possessed by a group do much to determine which targets can be attacked. However, the terrorists' capability is also affected by the ability of a group's leaders to motivate ordinary members and plan operations whilst the quality of their ordinary members determines whether their weapons and other resources are used effectively.[111]
- "Contemporary international terrorism is well suited to the technology of our era…Weapons and explosives are increasingly available, and modern industrial society presents many vulnerable targets."[112]

Logistical Resources

- "Logistics Network…consists of the support structure necessary to sustain [the group]…includes the means to transport weapons and personnel, to house members of the group without arousing suspicion, and generally to allow the group to function."[113]
- "…[S]ome terrorist groups set up a logistics network before they start using violence…Setting up a logistics network for one operation is only necessary when the operation itself is complex.[114]

---

[107] Bruce Schneier, *Secrets and Lies: Digital Security in the Networked World* (New York: Wiley, 2004), p. 53.
[108] Brian M. Jenkins, "Defense Against Terrorism," *Political Science Quarterly* 101:5, Reflections on Providing for "The common Good" (1986), p. 778.
[109] Drake, *Terrorists' Target Selection*, p. 95.
[110] *Ibid*, p. 93.
[111] *Ibid*, p. 97.
[112] Jenkins, "Defense Against Terrorism," p. 776.
[113] Drake, *Terrorists' Target Selection*, p. 54.

- "Although groups with few full-time members and relatively primitive weapons can function without a large base, more sophisticated groups need the money to pay for weapons and other resources such as ID and travel documents."[115]
- "Terrorism's trend toward increasing lethality is also a reflection of the fact that terrorists themselves are more adept at killing. Not only are their weapons becoming smaller, more sophisticated, and deadlier...but terrorists have greater access to these weapons through their alliance with foreign governments."[116]
- "Accordingly, irrespective of communist-bloc action, terrorists now are assured an almost inexhaustible international stockpile of plastic explosives on which to draw for future operations. Moreover, even those organizations lacking a government patron or sponsor can easily obtain a range of sophisticated weapons – including Semtex H – on the international black market."[117]

Analysis:

There is usually a more or less direct correlation between the resources available to a terrorist group and its ability to attack desired targets. However ambitious their targeting goals may be, groups with very few means will simply be unable to achieve them unless they can gain access to additional financial, physical, and logistical resources. Any support provided to them by states, usually covertly, will almost invariably come with strings attached, and these may in fact serve to constrain a terrorist group from attacking targets that it would otherwise be inclined to attack.

7) Operational Capabilities

There are a number of references in the literature to the operational capabilities of terrorist groups. These can be divided into four categories, three of which were identified as subfactors:

General

- "The terrorists' strategic options are also circumscribed by their capabilities…their material resources…[and the] abilities of their operatives. Terrorists may make misjudgments as to their capabilities and overreach themselves, …"[118]
- "…[T]errorists consciously learn from one another …"[119]
- "… [E]very new terrorist generation learns from its predecessors, becoming smarter, tougher, and more difficult to capture or eliminate."[120]
- there is normally a "relationship between simplicity and success…because terrorist organizations, similar to military units in combat, become vulnerable to factors outside their sphere of control as soon as the mission enters its executions phase."[121]

Technical Expertise

---

[114] *Ibid*, p. 55.
[115] *Ibid*, p. 97.
[116] Hoffman, *Terrorist Targeting*, p. 9.
[117] *Ibid*, p. 11.
[118] Drake, *Terrorists' Target Selection*, p. 178.
[119] Hoffman, "Modern Terrorist Mindset," p. 7.
[120] *Ibid*, p. 14.
[121] Palfy, "Weapons System Selection," p. 87.

- "The centrality of technology to all terrorist and counterterrorist operations represents an important incentive for individual groups to seek out and master new techniques and weapons"[122]
- "[T]he opportunities presented by the technological dependence of society will…be inaccessible unless terrorist groups master the techniques necessary to capitalize on them."[123]
- "…[I]t is relevant to reexamine the topic of technology and terrorism from a dynamic perspective by examining not what happens when terrorists gain a new technology but the steps and missteps that are taken as part of the acquisition process."[124]
- "…[A]ll individuals and groups do not absorb and successfully apply new technology at the same rate."[125]
- "There are two general mechanisms through which an organization can acquire new technology…*internal innovation*...[and] *external* sources of innovation." [126]
- "…[*E]xplicit knowledge* [is] information…that can be readily codified and set down in written form or embodied in a physical object…it is also readily transferred between one firm and another." In practice, of course, "it is often the case that even well understood technologies do not readily transfer into a firm and are not easily applied."[127]
- "In contrast, *tacit knowledge* is much more difficult to transfer among individuals or firms…[for example,] even if the company selling the equipment makes every effort to communicate its knowledge about usage, much of the tacit knowledge associated with the machine's operation will not be effectively transferred. As a result, the purchaser of a new technology will *always* have to go through a subsequent internal learning process where necessary tacit knowledge is "discovered" and the technology is adapted to the user's specific needs."[128]
- "A group with a greater knowledge of explosives and tacit understanding of where to place them for maximal effect…has arguably adopted the technology more completely…[this] group would pose a far greater threat and be more worthy of counterterrorist attention…variations in 'inherent complexity' will affect the ability of groups to successfully adopt techniques or devices."[129]
- "…[E]ven 'off-the-shelf" weapons, like a new machine purchased by a commercial firm, require the accumulation of tacit and experiential knowledge regarding their use."[130]
- "For terrorists wishing to carry out more complex operations, training in the use and construction of weapons is extremely useful."[131]
- "For groups seeking legitimacy and "respect" in today's technologically advanced world, the sophistication of a group's attacks can be of utmost importance. Such a distinction is important both for public reactions – where a more technological attack may result in greater impact – and in the ability of the terrorist group to gain the attention of the world press necessary to transmit their propaganda to a broad audience."[132]
- "This pressure to gain media attention and prominence has been suggested as one of the reasons why terrorist acts in recent years have gradually escalated in their scale and lethality. New technologies and weapons are absolutely necessary in the escalation and, as a result, the ability of a group to absorb and deploy them is a critical factor in determining the success of this escalation process."[133]

---

[122] Jackson, "Technology Acquisition by Terrorist Groups," p. 184.
[123] *Ibid*, p. 184.
[124] *Ibid*, p. 185.
[125] *Ibid*, p. 186.
[126] *Ibid*, p. 187.
[127] *Ibid*, p. 187.
[128] *Ibid*, pp. 187-188.
[129] *Ibid*, p. 196.
[130] *Ibid*, p. 197.
[131] Drake, *Terrorists' Target Selection*, p. 81.
[132] Jackson, "Technology Acquisition by Terrorist Groups," p. 185.
[133] *Ibid*, p. 185.

- Understanding this first level of the technology adoption process – controlled by the organization's 'desire for innovation' – is critical for assessing the likely technology trajectory of a group and is therefore a relevant starting point for a technology based terrorism threat assessment…Organizations, whether they are legitimate or underground, do not innovate for the sake of innovating. Rather, a company or terrorist group will choose to pursue a new piece of technology because of the belief that there is something to be gained by doing so."[134]
- "…[I]nternational cooperation…can lead to technology transfer among extremist groups…the direct communication and face to face contact generated by cooperation between firms have proven to be critical for the efficient transfer of expertise and tacit knowledge."[135]
- Schneier instead emphasizes "the ease with which successful techniques can propagate through cyberspace…The Internet is…a perfect medium for propagating successful attack tools."[136]

Propensity to Innovate

- "Terrorist tactics have remained relatively unchanged over time. When terrorists do innovate, it is only to overcome a specific countermeasure. Terrorists, unlike armies in conventional warfare, have virtually unlimited targets, and this reduces the requirement for tactical innovation. When confronted with security measures, terrorists merely alter their tactics to obviate the security measures of shift their sights to other vulnerable targets. Because terrorists can attack anything, anywhere, any time, and governments cannot protect everything, everywhere, all the time, terrorists always retain a certain advantage. Over the years the spectrum of targets attacked by terrorists has expanded. This asymmetry also means an inequality of effort between terrorist attackers and antiterrorist defenders. The amount of resources required for defense against terrorism is determined not by the very small number of terrorists, but rather by the virtually unlimited number of targets to be defended. This makes terrorism a cheap way to fight and a costly kind of threat to defend against."[137]
- Terrorists "are tactically conservative, preferring the weapons with which they are familiar. Rather than adopting entirely new techniques, most terrorists appear to prefer to adapt and improve their existing ones…"[138]
- "Terrorists have demonstrated repeatedly that their goals and objectives can be accomplished by using the same tactics and 'off-the-shelf-weapons' (though cleverly modified or adapted to their needs) that they have traditionally relied upon."[139]
- "Indeed it is not surprising to find that the frequency of various types of terrorist attacks decreases in direct proportion to the complexity or sophistication required…The fact that these percentages have remained largely unchanged for the past 25 years [this article was written in 1992] provides compelling evidence that the vast majority of terrorist organizations are not tactically innovative."[140]
- "…[E]xperience has nonetheless demonstrated repeatedly that, when confronted by new security measures, terrorists will seek to identify and exploit new vulnerabilities, adjusting their means of attack accordingly and often carrying on despite the obstacles placed in their path."[141]

---

[134] *Ibid*, p. 189.
[135] *Ibid*, p.199.
[136] Schneier, *Secrets and Lies*, pp. 21-22.
[137] Jenkins, "Defense Against Terrorism," pp. 777-778.
[138] Cameron, *Nuclear Terrorism*, p. 156.
[139] Hoffman, *Terrorist Targeting*, p. 15.
[140] *Ibid*, p. 2.
[141] Hoffman, "Modern Terrorist Mindset," p. 16.

- "Success for the terrorist is dependent not only on their ability to keep one step ahead of the authorities but of the counter-terrorist technology curve as well. The terrorist group's fundamental organizational imperative to act also drives this persistent search for new ways to overcome, circumvent or defeat governmental security and countermeasures."[142]
- "In hopes of obviating, or at least reducing, these risks, the P[rovisional]IRA's bombmakers invented a means of detonating bombs from a safe distance using the radio controls for model aircraft purchased at hobby shops. Scientists and engineers working in the British Ministry of Defence's (MoD) scientific research and development (R&D) division in turn developed a system of electronic countermeasures and jamming techniques for the Army that effectively thwarted this means of attack. However, rather than abandon this tactic completely, the PIRA began to search for a solution. In contrast to the state-of-the-art laboratories, huge budgets and academic credentials of their government counterparts, PIRA's own 'R&D' department toiled in clears beneath cross-border safehouses and backrooms of urban tenements for five years before devising a network of sophisticated electronic switches for their bombs that would ignore or bypass the Army's electronic countermeasures."[143]
- "But if past experience is any guide, as airport security and bomb detection technology closes off [one] avenue of attack, terrorists will not give up attacking airliners but merely find another means of doing so. They are likely to turn to readily available shoulder-fired, precision–guided surface-to-air missiles as the only practical means to attack commercial aircraft. A single terrorist, trained in the use of this weapon, could position himself at the edge of any airport's runway and fire at incoming or departing passenger planes. Indeed, on the few occasions in the past when guerrillas have targeted nonmilitary aircraft with surface-to-air missiles, they have had spectacularly devastating results."[144]

Specialized Skills

- "Those [terrorists] who used conventional high explosives had experience in combat."[145]

There is nothing in the literature that deals with other subfactors such as familiarity with the target environment, networking abilities, or knowledge of the target.

Analysis:

Obviously, the degree to which it is possible for a group to carry out terrorist attacks is dependent upon that group's operational capabilities. The extent of a group's capabilities also affects its choice of targets, since few groups knowingly select targets that they lack the abilities to attack successfully. *Terrorists generally tend to rely on tried-and-true weapons for the simple reason that they have worked so well in the past and continue to work well*, and for that reason some analysts have characterized terrorists as conservative. Yet there is not an urgent need to innovate as long as the employment of traditional techniques and weapons permit the achievement of one's objectives. *As countermeasures become more elaborate and sophisticated, however, terrorists are inevitably forced to expand their capabilities so that they can adopt new techniques and/or employ new, more effective weapons*. In that sense, there is an ongoing cycle of innovation, as those who seek to protect targets and those who seek to attack them try to outmaneuver each other.

---

[142] *Ibid*, p. 15.
[143] Hoffman, *Terrorist Targeting*, p. 12.
[144] *Ibid*, p. 14.
[145] John Parachini, "Comparing Motives and Outcomes of Mass Casualty Terrorism Involving Conventional and Unconventional Weapons," *Studies in Conflict and Terrorism* 24 (2001), p. 402.

Moreover, since terrorists feel a perceived need to demonstrate their prowess and thereby rally their supporters, frighten their enemies, and obtain publicity for their cause, they *are on the lookout for new technologies that might enable them to attack high-profile targets successfully*. Hence they make an effort to learn from previous experience and from one another, borrow techniques directly or indirectly, and acquire more knowledge about new weapons and techniques to do damage to their opponents. These activities are facilitated by the Internet, which means that it is no longer necessary for terrorists to obtain requisite knowledge from personal contacts with experts. Although in many cases there is still no substitute for getting hands-on training, it is now possible to obtain a vast amount of useful information online, which makes it easier for terrorists to adopt and adapt new methods and technologies. To the extent that they are able to do so, their range of potential targets can only increase.

8) Perceptual Filter

The following information details the major categories of potential bias mentioned in the literature:

General

- "…[*W*]*e construct* the reality in which we operate. We take our perception of the world for granted."[146] "The "transactional" school of perception has emphasized that perception is always a "choice" or "guess" about the real nature of the stimulus."[147]
- "Note that the perception of a stimulus is just as important as the stimulus itself. We never respond to the actual event or situation but to our view of it."[148]
- "…[C]omplex problems are more likely to be defined by the decision maker's beliefs, expectations, and cognitive and emotional predispositions than by the 'objective' attributes of the situation…in circumstances of information overload one may also be more likely to screen information and to respond in terms of personal predispositions…"[149]
- "…[T]he organization will "view" as reality whatever will help establish a consensus. The individuals in the organization will then have to respond in terms of this construction."[150]
- "The need for people to simplify the enormous amount of information they receive and the psychological pressures that result in motivated distortions mean that there will be serious discrepancies between the perceived and the actual environment…. As these processes continue over time, furthermore, errors are likely to be compounded, not corrected."[151]
- "The experimental evidence suggests that there are a number of respects in which people do not behave according to the assumptions and predictions of expected-utility theory."[152]
- "[W]hen motivated biases are at work, one cannot predict the person's perceptions from his general belief system."[153]

---

[146] Joseph DeRivera, *The Psychological Dimension of Foreign Policy*, James N. Rosenau, consultant, (Columbus, OH: C.E. Merrill Publishing Company, 1968), p. 21.
[147] *Ibid*, p. 20.
[148] *Ibid*, p. 31.
[149] Ole R Holsti, "Crisis Decision Making: Perspective from Four Levels of Analysis," *Behavior, Society and Nuclear War* 1, Philip E. Tetlock, et. al, eds. (New York: Oxford University Press, 1989), p. 33.
[150] DeRivera, *The Psychological Dimension of Foreign Policy*, p. 60.
[151] Jervis, Robert, "Perceiving and Coping with Threat," *Psychology and Deterrence* (Baltimore, MD: Johns Hopkins University Press, 1989), p. 33.
[152] Jack S. Levy, "Prospect Theory, Rational Choice, and International Relations," *International Studies Quarterly* 41:1 (March 1997), p. 89.
[153] Robert Jervis, "Perceiving and Coping with Threat," p. 32.

- "The fact remains that human beings, programmed as they are with emotions and unconscious motives as well as with cognitive abilities, seldom can approximate a state of detached affectlessness when making decisions that implicate their own vital interests or those of their organization or nation…we can say that thinking about vital, affect-laden issues generally involves *hot* cognitions, in contrast to the cold cognitions of routine problem solving."[154]

Risky Shift

- "Some experiments suggest that groups are more prone [than individuals] to choose high-risk options and that group discussions are likely to cause individuals to shift to riskier choices."[155]

Ambiguity under Stress

- "These biases arise because the problem of dealing with complex and ambiguous information leads people to adopt short-cuts to rationality that simplify perceptions in order to make more manageable the task of making sense out of environments."[156]
- "…[I]t is not practical for the real-world decision maker to take the time and effort to make optimal choices…"[157]
- "…[A]mbiguity abets instinct and allows intuition to drive analysis. The greater the ambiguity, the greater the impact of preconceptions."[158]
- "…[W]hen stress increases, problem solving tends to become more rigid: the ability to improvise declines; previously established decision rules are adhered to more tenaciously, whether appropriate to the circumstances or not…"[159]

Analogy and Cognitive Dissonance

- Events that are seen firsthand, that happen early in the person's adult life, and that affect him and his country have great impact on his later perceptual predispositions.
- Because outcomes are learned without careful attention to details of causation, lessons are superficial and overgeneralized. Analogies are applied to a wide range of events with little sensitivity to variations in the situation.
- "The perception that actually occurs is the one that requires the least reorganization of the person's other ideas."[160]
- "[D]ecision-makers do not examine a variety of analogies before selecting the one that they believe sheds the most light on their situation. Instead, because of their predispositions, they see the present as like recent and dramatic events without carefully considering alternative models or the implications of this way of perceiving. They thereby fail to apply fully their intelligence to some of the most important questions they face."[161]

---

[154] Irving L. Janis and Leon Mann, *Decision Making: A Psychological Analysis of Conflict, Choice, and Commitment* (New York: The Free Press, 1977), p. 45.
[155] Holsti, "Crisis Decision Making," p.19
[156] Jervis, "Perceiving and Coping with Threat," p. 18.
[157] Holsti, "Crisis Decision Making," p. 22.
[158] Richard K Betts, "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable," *World Politics* 31:1 (Princeton University Press, October 1978), p. 70.
[159] Holsti, "Crisis Decision Making," p. 32.
[160] DeRivera, *The Psychological Dimension of Foreign Policy*, p. 22.
[161] Jervis, *Perception and Misperception in International Politics* (N.J.: Princeton University Press, 1976), pp. 281-282.

- " [T]he lessons people learn are usually oversimplified and overgeneralized—they expect the future to resemble the past."[162]
- "[P]ropensities to assimilate and interpret incoming information in ways that conform to, rather than challenge, existing beliefs, preferences, hopes, and expectations; denial of, rather than acceptance of, the need to confront trade-offs; and postdecision rationalizations to bolster the selected options while denigrating those that were rejected…"[163]
- "Bolstering is accomplished partly by magnifying the attractiveness of the chosen alternative—the gains to be expected are played up and the potential losses are played down…the chosen course of action comes to be regarded more highly and each unchosen alternative is regarded less highly…*Exaggerating favorable consequences… Minimizing unfavorable consequences… Minimizing personal responsibility*." [164]

Groupthink

- " 'Groupthink'—defined as a deterioration of mental efficiency, reality testing, and moral judgment—occurs when concern for group solidarity supersedes the effective performance of vital decision-making tasks."[165]
- "Extensive evidence indicates that interaction within groups reduces variance in behavior, crystallizes attitudes and beliefs, and generally exerts pressures for conformity to group norms."[166]
- "…[A] prime example of concurrence-seeking tendency that has been observed among highly cohesive groups. When this tendency is dominant, the members use their collective cognitive resources to develop rationalizations supporting shared illusions about the invulnerability of their organization or nation and display other symptoms of "groupthink"—a collective pattern of defensive avoidance."[167]
- The symptoms of groupthink can include "an illusion of invulnerability, shared by most or all of the members, which creates excessive optimism and encourages taking extreme risks;… an unquestioned belief in the group's inherent morality, inclining the members to ignore the ethical or moral consequences of their decisions;… stereotyped views of rivals and enemies as too evil to warrant genuine attempts to negotiate, or as too weak or stupid to counter whatever risky attempts are made to defeat their purposes;… self-censorship of deviations from the apparent group consensus, reflecting each member's inclination to minimize to himself the importance of his doubts and counterarguments;… a shared illusion of unanimity, partly resulting from this self-censorship and augmented by the false assumption that silence implies consent."[168]

Attribution Error

- "[T]he basic attribution error—a tendency to explain the adversary's behavior in terms of personal characteristics…instead of the context or situation, while attributing one's own behavior to the latter…instead of the former."[169]

---

[162] Robert Jervis, "Perceiving and Coping with Threat," *Psychology and Deterrence* (M.D.: Johns Hopkins University Press, 1989), p. 22.
[163] Holsti, "Crisis Decision Making," p. 23.
[164] Janis and Mann, *Decision Making,* pp. 82, 91.
[165] Holsti, "Crisis Decision Making," p. 21.
[166] *Ibid*, p. 19.
[167] Janis and Mann, *Decision Making,* p. 129.
[168] *Ibid*, pp. 130-131.
[169] Holsti, "Crisis Decision Making," pp. 23-24.

Analysis:

Perceptual biases (whether cognitive or affective) are ubiquitous when it comes to decision-making. However, in the case of terrorist groups, which are often isolated, under varying levels of stress and already have radical and violent outlooks, these features are believed to be especially prominent. We have attempted to capture all the abovementioned effects, by representing them under the broad rubric of a perceptual filter. The perceptual filter serves as a construct that acts on all information flows into and within the terrorist group. Specific effects can include:

- Cognitive dissonance, where information contrary to decision-makers' preconceptions and beliefs is ignored or understated.
- Attribution bias, where enemy actions are perceived one way (such as being the result of malice), while group actions are viewed as complex and arising from numerous influences. Another form of attribution bias is one in which the group views its past successes as the result of its own capabilities, while past failures are attributed to misfortune.
- Maladaptive analogizing, where decision makers interpret current events and stimuli by fitting them into heuristics they have developed over time, but which may distort the objective truth significantly.
- Groupthink, where through a variety of mechanisms, groups converge on consensus to preserve group solidarity at the expense of optimal decision making.

Including the perceptual filter helps to inform analysis by highlighting the impact of perception on terrorist decision-making, and specifically on target selection. While the literature does not discuss this aspect directly, it is often implicit in the discussion of other factors.

Factors External to the Group

9) Historical Events

There is nothing in the literature specifically dealing with the impact of historical events on terrorist group targeting. However, to the extent that historical factors play a role in conditioning a group's ideological views, they are very significant indeed, since, as has been noted above, ideology is probably the single most important factor influencing target selection. Hence the following points deserve emphasis:

- [T]errorist groups often inherit or adopt pre-existing "scripts" or ideas rather than creating brand new ones *sui generis*.[170]
- [H]istorical precedents and the "(interpreted) experiences of their predecessors" can serve as attractive guides to terrorist action.[171]
- "It may be, for example, that…the anniversary of an event would be a sufficient destabilizing factor to raise the level of concern" by increasing a group's "sense of urgency" and thereby its "propensity for violence." Do group members "perceive this event to be [such] a turning point with regard to key points in their ideology that something needs to be done, that this is the time to act…?"[172]

These are the only references to historical factors in the literature, although they address terrorist targeting only indirectly.

---

[170] McCormick, "Terrorist Decision Making," p. 488.
[171] *Ibid*, p. 488.
[172] Pynchon and Borum, "Assessing Threats of Targeted Group Violence," p. 348.

Analysis:

The importance of existing ideas and historical precedents in influencing terrorist behavior must be recognized. No terrorist group emerges from the ether with an entirely blank slate, since its members have invariably internalized, adopted, or adapted and modified many pre-existing ideas. Likewise, no newly-emergent terrorist group is entirely unaware of the methods and tactics employed by prior or existing terrorist groups, especially those that have operated within its own political, intellectual, ethnic, religious, or cultural milieu. Hence those *precedents, even if they do not consciously serve as exemplars or models, are bound to exert some degree of influence on a group's target selection and modus operandi*. It goes without saying that past events that are viewed as having great significance may well affect a group's decisions about who and what to target and when to launch attacks. The past is rarely entirely forgotten – however idealized and distorted – even in the context of terrorist targeting.

10) Relations with External Actors

There are a number of references in the literature to the impact of a terrorist group's relations with external actors on its target selection. These external actors need to be divided into several categories, including the all-important target audience, possible state sponsors, and other external groups:

General

- "The terrorist campaign is thus like a shark in the water: it must keep moving forward – no matter how slowly or incrementally – or die. Hence, when these more 'typical' targets fail to sustain the momentum of a terrorist campaign or when other, perhaps even totally unrelated events overshadow the terrorists and shunt their cause out of the public eye, terrorists often have to resort to more violent acts to dramatically refocus attention back upon themselves."[173]
- "However, for Carlos [the Jackal] and [Ramzi] Yousef as for many other terrorists, this equation of publicity and attention with success and self-gratification has the effect of locking them onto an unrelenting upward spiral of violence in order to retain the media and public's attention."[174]
- "The more successful…terrorist organization, therefore, 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 modulated so as not to provoke massive governmental crackdown and reaction."[175]

Target Audience(s)

- "[Terrorist groups'] tactical and targeting choices correspond to, and are determined by, their respective ideologies, attendant mechanisms of legitimization and justification and, perhaps most critically, by their relationship with the intended audience of their violent acts."[176]
- "As the PFLP's Bassam Abu Sharif explained, 'For violence to become fruitful, for it to get us to our aims, it should not be undertaken without a proper political base and intention.' While the logic in such a case may well be contrived, there is nonetheless a clear appreciation that violence has it limits and, moreover, if used properly, it can pay vast dividends. In other words, the level of violence must be kept within the bounds of what the terrorists' 'target audience' will accept…But acts of terrorism, like battles in conventional wars, are difficult to limit and control once they are started…"[177]

---

[173] Hoffman, "Modern Terrorist Mindset," p. 4.
[174] *Ibid*, p. 13.
[175] *Ibid*, p. 4. This particular comment was specifically made in reference to ethno-nationalist and separatist terrorist organizations, but it undoubtedly has a broader application.
[176].*Ibid*, pp. 1-2.
[177] *Ibid*, p. 5.

- "Mao suggested that guerillas must aim for and depend upon the political mobilization of people who would be mere bystanders in a conventional military conflict. He introduced a relationship between military action and the attitude and response of the audience that added a new dimension to armed conflict: instead of gauging success primarily in terms of the physical effect that military action had on the enemy, strategists could now say that the effect of a violent action on the people watching may be independent of and may equal or even excel in importance the actual physical damage inflicted on their forces. Terrorism is that proposition pursued to its most violent extreme."[178]

State Sponsors

- "The influence of foreign sponsors on the selection of terrorist targets has varied."[179]
- "Growing state sponsorship of terrorism has serious consequences. It puts more resources in the hands of the terrorist: money, sophisticated munitions, intelligence, and technical expertise. It also reduces the constraints on terrorists, permitting them to contemplate large-scale operations without worrying about alienating perceived constituents or provoking public backlash, since they need not depend on the local population for support…Without the need to finance themselves through bank robberies or ransom kidnappings and without the need to carry out operations just to maintain group cohesion, state-sponsored terrorist groups operate less frequently than groups that receive little or no state support, but they are many times more lethal and have far greater operational reach."[180]
- "State sponsorship, in particular, could provide terrorists with the incentives, capabilities, and resources they previously lacked for undertaking an ambitious operation in any of these domains. Combined with intense ethnic enmity of a strong religious imperative, this could prove deadly."[181]
- "…[T]errorist acts by groups that are state sponsored have been shown, on average, to be eight times more lethal than those by groups without sponsors; although this difference was ascribed to the access to armaments and technologies made available by the state sponsors, it is relevant to consider the effects that state sponsorship can have on the groups' adoption of the technologies as well."[182]

Miscellaneous External Actors

- "Being familiar with sources of support is important because they offer clues to the group's intentions. When a group actively seeks or receives the support of regimes or organizations with a known violent purpose, the risk that the radical group will itself embark on the pathway to violence and terrorism increases. In addition, the likelihood increases that the targets of violence will shift to align with the goals of the group's benefactors."[183]
- "Furthermore, a group's constituents or supporters can either deter or encourage terrorist activity. The observable indicators [are]:
    A. The group receives support from a source or sources with a known violent agenda (e.g., a hostile state or a terrorist group, such as Iran's support of Hizbullah:
    B. Supporters or constituents of the group exert pressure on the group to take violent action (e.g., by threatening to withdrawer or shift support).
    C. Supporters or constituents provoke violence, forcing the group to act.
    D. Foreign or other influential supporters order the group to undertake terrorist operations."[184]

---

[178] Jenkins, "Defense Against Terrorism," p. 776.
[179] Drake, *Terrorists' Target Selection*, p. 90.
[180] Jenkins, "Defense Against Terrorism," p. 778.
[181] Hoffman, *Terrorist Targeting*, pp. 16-17.
[182] Jackson, "Technology Acquisition by Terrorist Groups," p. 199.
[183] Post, Ruby, and Shaw, "Radical Group in Context," p. 83.
[184] *Ibid*, p. 83.

- "…[S]upport could stop if [terrorist groups] frequently overstep the boundaries of what is deemed by their supporters or potential sympathizers to be acceptable behavior. Thus, as well as providing support, the relationship places limits on the activities of the group."[185]

Analysis:

It is clear that *terrorists, if they wish to achieve the effects that their violent attacks are specifically intended to have, must carefully take into account the opinions of external actors when selecting targets. This is above all the case in terms of the target audience at whom the attacks are directed,* as opposed to the victims per se, since that audience must receive the message that the perpetrators intend to convey or their act of violence will be meaningless if not counterproductive. However, *they must also take into account the reactions of their supporters and sympathizers, their potential constituents, other extremist groups in their area, and – if they have them – sponsoring states*. Needless to say, carrying out acts of violence which have the effect of alienating the terrorists' own support base would be foolish, and to the extent that they are dependent upon external support from states, however covert that support may be, they cannot afford to take actions that those state sponsors will strongly disapprove of. In short, since terrorism is violence for psychological effect, the terrorists have to be very concerned about the effects their acts have on others. This will necessarily affect their selection of targets, and also often the level of violence they decide to employ.

11) Security Environment

There are very few direct references to the security environment in the literature and almost none in connection with terrorist target selection:

- Terrorists usually consider several targets before making a final decision, and have "often made final decisions about whom to attack because an opportunity for attack presented itself or because they perceived another target was unapproachable."[186]
- A group such as al-Qa`ida will "follow the path of least resistance" in its operational planning and target selection, since "the flow of al-Qaeda terrorism activity is towards weapon modes and targets, against which the technical, logistical and security barriers to mission success are least."[187]
- "Advances in technology and, more specifically, the interconnectedness and interdependencies they entail have…made modern society increasingly more vulnerable to terrorism." Examples include transportation systems, trade and product distribution systems, power generation and water networks, and the Internet.[188]

Analysis:

There is no doubt that the nature of the security environment will affect terrorist target selection. After all, it is impossible for the authorities to protect every conceivable target at all times, especially in democratic, target-rich industrialized societies, and terrorists will likely be monitoring security arrangements closely to determine which targets offer the most "bang for the buck," i.e., the best combination of symbolic or instrumental value and vulnerability. *Dedicated terrorists will rarely if ever cease planning and launching attacks, no matter how tough the overall security environment becomes*.

---

[185] Drake, *Terrorists' Target Selection*, p. 148.
[186] Robert A Fein and Bryan Vossekuil, *Protective Intelligence and Threat Assessment Investigations: A Guide for State and Local Law Enforcement Officials* (Washington, DC: US Department of Justice, 1998), p. 20.
[187] Gordon Woo, "Quantitative Terrorism Risk Assessment," Risk Management Solutions report, p. 7: http://www.rms.com/NewsPress/Quantitative Terrorism_Risk_Assessment.pdf.
[188] Jackson, "Technology Acquisition by Terrorist Groups," p. 184.

However, they may not always be aware of major or minor changes in the security environment and, by extension, may not correctly assess the vulnerabilities of selected targets, whether as a result of ideological fanaticism, perceptual blinders, or faulty surveillance, and if so they may well make mistakes in their targeting. Moreover, they may not always have the necessary resources or capabilities to attack even vulnerable targets successfully. Yet it is their perception of the security environment, whether or not this reflects its true condition, that affects target decisions.

12) CI Characteristics

There are several references to the effects that the actual characteristics of the target, CI or otherwise, have on terrorists' decisions to attack. These fall under several rubrics that, in most cases, roughly correspond to the subfactors for this category.

General

- "…[A] terrorist or aggressor will analyze the building or target … to determine the type of attack, type of weapon, and tactics to employ to defeat the building or critical mission/business function."[189]

Level of Protection

- Schneier uses the term "vulnerability landscape" to describe the level of a system's vulnerability to attack, and says that this "vulnerability landscape" can be organized into the physical world (i.e., physical attacks), the virtual world (digital and cyber attacks), the trust model (insider problems), and the system's life cycle.[190]
- Terrorists are likely to attack less protected targets if the protective measures around primary targets are hardened.[191] For example, the fence perimeter around the US consulate in Bali forced the terrorists to look for a softer target, in this case a night club, and the adoption of protective body armor by British soldiers caused the IRA to attack more vulnerable targets.[192]
- The provision of better protection for a building will decrease its chances of being attacked, and a building built to withstand attacks will likely suffer minimal damage even if it is attacked.[193]
- Some CI facilities, such as nuclear power plants, possess inherent "hardness" since they have strong buildings, reinforced doors, and structural strength. Such facilities may well be less vulnerable to terrorist attack even though they might seem to be an ideal target for a terrorist attack.[194]
- Increased protection restricts a terrorist group's options. For example, although Aum Shinrikyo was able to get away with conducting small CBW operations and tests, increases in security resulting from a greater awareness of the threat would have posed greater risks for them at a later date.[195]

---

[189] FEMA, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings* (Washington, DC: FEMA, 2003), Department of Homeland Security Risk Management Series, chapter 1, p. 22.
[190] Schneier, *Secrets and Lies*, pp. 282-287.
[191] Gordon Woo, "The evolution of Risk Modeling," *Journal of Reinsurance* (April 2003), pp. 6-7. Cf. Drake, *Terrorists' Target Selection*, p. 117. Cf. Philip Anderson, *Threat-Vulnerability Integration: A Methodology for Risk Assessment* (Washington, DC: Center for Strategic and International Studies, no date [2002?]), p. 6; and Nancy A. Renfroe and Joseph L. Smith, "Threat/Vulnerability Assessments and Risk Analysis," Whole Building Design Guide website, p. 2: http://www/wbdg/org/design/res-print.php?rp=27.
[192] Woo, "Understanding Terrorism Risk," pp. 8- 9.
[193] FEMA, *Reference Manual to Mitigate Potential Terrorist Attacks*, chapter 1, p. 21.
[194] Anderson, *Threat-Vulnerability Integration*, p. 6.
[195] Jackson, "Technology Acquisition by Terrorist Groups," p. 203.

- Better protection of facilities may obviate the need for good detection and reaction mechanisms.[196]
- Conversely, effective alarm systems and surveillance mechanisms might serve to deter terrorists from attacking a target, since such systems will prevent a fast and easy penetration of its defenses.[197]
- Increased target protection is unlikely, however, to deter suicide attackers.[198]
- The level of target protection influences the operational planning for an attack. An increase in the security level for a facility might force terrorists to invest more time and money so as to overcome these increased security measures.[199]
- Increased security measures might also lead terrorists to adopt other highly destructive tactics in order to overcome such protective mechanisms. For example, terrorists might use a guided missile to destroy a highly protected airport which seemed impregnable to attacks by vehicles or human agents.[200]
- The level of protection of a target also affects the desired effects of the attack. A terrorist group might proceed to attack a well hardened target precisely in order to display its strength and capabilities, garner increased publicity, and advance the group's cause by carrying out a difficult and successful task.[201]

Profile of Target

- The public profile of a target affects the selection of targets. Drake observes that terrorists are less likely to attack targets that are less known among the public.[202]
- Targets with a high symbolic value or utility are more attractive to terrorists, and a target's attractiveness increases its likelihood of being attacked.[203]

Function of Target

- The function and affiliation of a particular target influences a terrorist group's target selection. For example, a person opposed to the government is more likely to attack a federal building than a multi-tenant office building.[204]

Target Value

- The projected political, economic, and military costs a nation will suffer due to the destruction of, or damage inflicted on, particular targets plays an important role in terrorist target selection. Renfroe and Smith refer to this as "impact loss," and posit that a target with both a high impact loss and a high degree of vulnerability would be an ideal choice for terrorists.[205]
- FEMA has developed a 10-point impact scale taking into account the human and economic loss inflicted as a result of an attack. A value of 10 signifies a large number of human casualties and a major loss of core functions of the facility.[206]

---

[196] Schneier, *Secrets and Lies*, p. 280.
[197] Drake, *Terrorists' Target Selection*, pp. 103, 108.
[198] *Ibid*, p. 115.
[199] *Ibid*, p. 111.
[200] Jackson, "Technology Acquisition by Terrorist Groups," p. 208.
[201] Drake, *Terrorists' Target Selection*, pp. 111-112, 119.
[202] I*bid*, p. 98.
[203] Renfroe and Smith, Threat/Vulnerability Assessments and Risk Analysis," p. 1-2.
[204] *Ibid*, p. 1.
[205] *Ibid*, pp. 1-2.
[206] FEMA, *Reference Manual to Mitigate Potential Terrorist Attacks*, chapter 1, pp. 13-14.

Target Location

- The location of a target relative to the terrorists' base might affect the operational planning for a particular attack. A target that is not in the same area as that of the terrorists' base might prompt the terrorists to use off-the shelf weapons systems and delivery systems for carrying out a particular attack.[207]

Analysis:

The characteristics of particular targets, including CI facilities, are usually the most important factors in a terrorist group's decision to attack – or not attack – those targets. No single characteristic of a facility is likely to determine its potential for being attacked. Instead, the totality of that facility's characteristics will normally influence the terrorists' decision about whether or not to attack it. The most important characteristics of a facility that may affect terrorist targeting are its level of protection, whether or not it has a high profile (which is in part a function of how much media attention it has received), and its actual function. The level of security at a facility is a particularly important factor, since it not only plays a role in the selection of targets but also in the attackers' operational planning. All things being equal, terrorists are more likely to select targets that are vulnerable. At the same time, they wish to attack functionally important, high-profile targets whose destruction will be costly to the host society. Hence a *key decision-making factor is usually the relationship between a facility's vulnerability and its desirability as a target*. Given the large number and wide range of potential targets, terrorists will tend to avoid heavily-fortified or heavily-protected targets unless these have extraordinary significance, and instead attack more vulnerable targets. Thus, *if certain targets are protected so well that they discourage or effectively prevent terrorists from attacking them, then others that are less well-protected will be more likely to be attacked*. These factors are applicable to all potential terrorist targets, including those that can be categorized as CI.

A few additional observations can be made. First, increased physical protection of targets increases the costs ofwould-be attackers and in some cases deters them from launching attacks. Second, the public profile of highly critical CI should, whenever possible, be kept at very low levels, although a CI facility whose functioning requires constant interface with the public unfortunately cannot escape publicity. Third, if it is not possible to provide protection to particular facilities all of the time, random rotations or alterations of security measures can serve to disrupt the terrorists' plans for an attack. Fourth, *a CI facility with extraordinary symbolic value is more likely to be attacked than a CI facility with high utility but less symbolic value*. However, targets with low symbolic value but unique abilities to impact society (such as a chemical factory that could release highly toxic chemicals) can still be attractive targets. Finally, the level of networking and degree of "embeddedness" of a particular terrorist group might play an important role in its ability to carry out attacks on CI facilities that are not located close to its own operational bases.

Decision-Making Factors

13) General Planning Characteristics

There is very little in the literature that relates specifically to the subfactors we have included under this rubric. The most relevant passages suggest that:

[207] Woo, "Understanding Terrorism Risk," p. 14.

Decision-Maker Time Horizon

- Terrorist decision-makers working in accordance with a specific timetable – even if it is a self-imposed deadline, as in the case of certain apocalyptic groups who anticipate the onset of Armageddon on a particular date – may feel the need to perpetrate more ambitious attacks, whether punitive or coercive in nature. Crackdowns by the security forces can also lead to a sense of urgency: "if a group feels that it will be in danger in the near future, it may be more likely to engage in terrorism due to a decrease in the range of perceived options. A group may be more likely to attack if it perceives a threat to group members or leaders, feels that the regime or other opponent is trying to destroy it, or becomes paranoid and defensive and attacks suspected traitors."[208]
- "An increased sense of urgency within the group may impact a group's propensity for violence, by (i) increasing the likelihood of an irrational reaction…; (ii) increasing the likelihood of flawed decision-making regarding targeted violence; or, (iii) decreasing the group's ability to see any non-violent alternative as a viable option."[209]

Risk Threshold

- Sophisticated, high-impact conventional and CBRN attacks generally require longer incubation periods than low-impact conventional attacks. For example, "the 1993 World Trade Center bombing was preceded by five months of preparations; the Aum Shinrikyo attack in 1995 was preceded by attempts that lasted for about a year; the 1995 Oklahoma City bombing plot began six months earlier; the Cole attack was reportedly planned for eight or ten months…and the 9/11 attacks were preceded by a two-year incubation period. Conventional, low-impact attacks are prepared quickly, generally in less than a week, so there is a much shorter window of opportunity to preempt such attacks."[210]
- In certain cases, once a group decides on a general category of targets, they will attack as soon as a specific target within that category presents itself.[211]

Analysis:

Two lessons can be drawn from the above. First, the specific operational objectives set by the group during the attack planning process can have an obvious and direct effect on the decision maker's time horizon, in that certain of these objectives may be time-dependent. An illustrative example could be a case in which a terrorist decision-maker wants to act to increase his group's recruitment vis-à-vis a rival organization: if he delays too long, his competitors may well end up inducting the best personnel from among the pool of available recruits and his goal of increasing recruitment may remain unfulfilled – no matter how successful the attack ultimately turns out to be. Second, the degree of risk that a group is willing to take in order to conduct any single attack is an important factor in the setting of operational objectives. *All else being equal, the greater the risk tolerance of a group when planning an attack, the greater the scale of the attack is likely to be*. A corollary to this is that the more wedded the group is to the success of an attack and its own preservation (i.e., the lower its risk tolerance), the more conservative its operational objectives will tend to be. Risk tolerance is a function of the group's ideology and the external environment, as well as other variables.

---

[208] Post, Ruby, and Shaw, "The Radical Group in Context," pp. 94-95.
[209] Pynchon and Borum, "Assessing Threats of Targeted Group Violence," p. 348. By extension, a sense of urgency may also prompt the group to carry out more extreme violence.
[210] Transcript of Presentation by Dr. Joshua Sinai, in "ICT Conference: Expert on Value, Methods of Forecasting Terrorist Incidents," *FBIS* #GMG20031202000085 Israel, 9 September 2003, p. 3.
[211] Drake, *Terrorists' Target Selection*, p. 56.

14) Operational Objectives

There is a good deal in the literature that deals with operational objectives. The relevant material has been divided into several sections, including:

General

- Operational objectives help to prioritize targets. Drake, who defines strategy as shaping the translation of political objectives into concrete actions,[212] maintains that "the range of targets is refined by the strategy of the group concerned. This is important because by its nature, terrorism is a method which – with the exception of expressive attacks – is intended to yield certain benefits by causing people to react to violence or the threat of violence."[213]
- "Whilst ideology sets out the range of people and things which it is legitimate for the terrorists to attack, the strategy sets out those targets which the terrorists believe it will be beneficial for them to attack. This does not mean that the terrorists will make the right decisions in this area, and whether their strategic choices actually prove to be beneficial is a task for hindsight and historians."[214]
- Operational objectives actively further ideological goals. This can be inferred from Fein and Vossekuil, who cite a study called the "Exceptional Case Study Project" (ECSP) that addresses the issue of assassins of public figures and concludes that an individual's motives and selection of a target are directly connected.[215]
- "The key point is that terrorism is growing in its lethality. How individual groups achieve that is partly an instrumental decision, based on the objectives of the group, and partly a matter of opportunism."[216]
- Both escalatory and moderating factors may affect the operational objectives of terrorists.[217]

Symbolic vs. Instrumental

- Terrorist targets are often chosen for their symbolic value rather than absolute military utility. By symbolic we mean that the target has a cultural or social meaning beyond its function or physicality that can be exploited to psychologically influence a terrorist's intended audience(s). Terrorist targets are often "deliberately selected and meticulously targeted for their intrinsic "symbolic" value."[218]
- "Symbolic targets are those where the primary motive for the attack is to prompt a reaction in the psychological target. This can be for a number of purposes. Terrorists may attack a target so as to draw attention to the group and their cause." However, "targets do not have to be prominent in order to have a symbolic value."[219]

[212] *Ibid*, p. 176.
[213] *Ibid*, p. 181.
[214] *Ibid*, p. 177.
[215] Fein and Vossekuil, *Protective Intelligence and Threat Assessment Investigations*, p. 15.
[216] Cameron, *Nuclear Terrorism*, p. 162.
[217] *Ibid*, pp. 156-157.
[218] Hoffmann, "Modern Terrorist Mindset," p. 2.
[219] Drake, *Terrorists' Target Selection*, p. 10.

Publicity

- Although publicity is important, terrorist violence is still calculated and calibrated to achieve political objectives. "Publicity and attention are of course paramount aims; but at the same time there is a conscious recognition that only if their violence is properly calculated and in at least in some (however idiosyncratic) way regulated, will they be able to achieve the effect(s) they desire and the political objectives they seek."[220]
- "A terrorist contemplating an assault on nuclear waste shipments could be looking for the actual or symbolic value in attacking such materials. The enormous disruption to normal public activities, a resulting sense of social panic, and/or the symbolic value of attacking the powerful federal government are but a few of the potential objectives for such an attack."[221]

Organization Building Effects

- "High-profile violence can be a means of reshaping popular perceptions about 'who's on top.' This, in turn, has two effects on mobilization: to boost popular confidence in the opposition and to diminish popular confidence in the state."[222]
- Attacks can be used to acquire or protect resources, which are referred to as "logistical targets" by Drake. "Logistical targets are those targets which are attacked in order to safeguard the group's resources."[223] He also refers to endorsement objectives: "*Endorsement:* attacks aimed at gaining endorsement are calculated to mobilize support for the group concerned."[224]

Punitive Effects

- Punitive operational objectives such as reaction and revenge also exist. "Terrorism can be an emotional response to a situation, rather than a part of an overall strategy…Lubsha cites indignation as a possible motive for carrying out an act of political violence. He defines indignation as an attitude and behavioral manifestations of wrathfulness because of unworthy or unjust treatment." "Revenge can also be a major motivation for specified attacks."[225]
- "…Yousef wanted to punish Americans for their government's support of the state of Israel. Once Americans suffered in the way Yousef believed Palestinians had suffered, then they would force their government to stop supporting Israel. Yousef also wanted to kill Americans so they would know the pain Arabs experienced. Moreover, he reasoned, maybe Americans would understand that their lives are no better than Arab lives. And finally, in the letter that Yousef and his co-conspirators sent to New York newspapers, they claimed that they represented a much larger movement, which had never been heard of before and has never been heard from since. Ramzi Yousef was not just striking out at the U.S. government, but he was seeking to kill individual American citizens because their death would cause the American people to understand the injustice that he believed Arabs suffered from Israel and the U.S. government."[226]

---

[220] Hoffmann, "Modern Terrorist Mindset," p. 8.
[221] James David Ballard, *A Preliminary Study of Sabotage and Terrorism As Transportation Risk Factors Associated With The Proposed Yucca Mountain High-Level Nuclear Facility* (Carson City, NV: Agency for Nuclear Projects, 1998), p. 4.
[222] McCormick, "Terrorist Decision Making," p. 485.
[223] Drake, *Terrorists' Target Selection*, p. 12.
[224] *Ibid*, p. 42.
[225] *Ibid*, pp. 14-15.
[226] Parachini, "Comparing Motives and Outcomes of Mass Casualty Terrorism," pp. 391-392.

Coercive Effects

- "The strategic objectives which [terrorists] set for themselves affect the targets which they choose because they hope that by attacking such targets, they will maximize the pressure upon the psychological target to behave in a certain fashion."[227]
- Drake has prepared a list of the psychological reactions sought by terrorists, four of which can be considered coercive in nature, whereas "threat elimination" limits the enemy's capability (but may be in part coercive), "advertisement" is linked to obtaining publicity, and "endorsement" has to do with organization-building. The four coercive ones are "compliance," "disorientation," "attrition," and "provocation." Here is his summary description of these: "Compliance occurs when the physiological targets obey the will of the terrorist group for fear of attacks upon themselves or upon people or objects of value to them…The strategic objective of disorientation can be differentiated from that of compliance in that with the latter one can obtain relief from fear by complying with the terrorists' demands, but with the former there is no certain course of action which will relieve the anxiety…A strategic objective of attrition is one where the terrorists intend to erode the will of the psychological target by attacking physical targets on which the psychological target sets some value. Whilst not precluding large-scale attacks, the emphasis of such a strategy is upon a continual series of small-scale attacks in the hope that cumulatively these will break the psychological target's resistance." [228]

Decreasing Enemy Capability Effects

- "*Functional targets* are people or objects whose destruction removes a threat to the terrorist group. The most obvious example would be the case of a terrorist being confronted by an armed opponent where he had to either kill the opponent or risk being killed or apprehended…the threat need not be so immediate. Police or intelligence officers who are involved with the investigation of terrorist groups are a prime target."[229]

Publicity Effects

- "[T]errorists wishing to gain publicity for their cause will not progress far if they confine themselves to minor acts of sabotage against unimportant buildings or institutions. Therefore they will select targets where attacks will gain attention."[230] Indeed, "…some terrorists carry out operations where the primary aim is the maximization of publicity."[231]

Provoking State Repression

- "Provocation occurs where the terrorist group carries out attacks in the hope of making the psychological target act in a way which will alienate people who were previously uncommitted, or possibly even unsympathetic towards the terrorists, as well as people who sympathizes with them."[232]

---

[227] Drake, *Terrorists' Target Selection*, p. 53.
[228] *Ibid*, pp. 39-43. These terms are meant to describe the type of reactions that the wider target audience of the terrorists is supposed to feel, and it may be very useful in some contexts. Since the current framework focuses more on the physical and social effects of an attack (seeking cues to indicate a critical infrastructure target), we prefer to use a classification that includes the latter aspects and thus will not dwell on the differences between, say, disorientation and compliance.
[229] *Ibid*, p. 11.
[230] *Ibid*, p. 39.
[231] *Ibid*, p. 42.
[232] *Ibid*, p. 41.

- "Terrorism, as [Menachem] Begin well understood, can also be employed to provoke. Terrorists, as a general rule, begin the game with the ability to see their opponents but a limited ability to attack what they see. The state, by contrast, begins the game with a much greater ability to attack what its sees but a limited ability to see what it wishes to attack. Terrorist groups enjoy an information advantage; the state enjoys a force advantage."[233]

High Profile vs. Low Profile Targets

- "Pot-boilers which in the rest of the study are termed irritants, are low-level attacks where the aim is to cause inconvenience and aggravation as a niggling reminder to the psychological target or targets that the terrorists are a problem which will not go away until they have got what they want. The aim of irritants is to keep up a constant minimum level of aggravation and inconvenience. Spectaculars are attacks intended to cause serious damage and distress."[234]
- "The exposure (and associated political attention) that a group receives is directly related to the shock effects of its attacks. To achieve these effects, terrorists continue to look for an edge, tactically and technically, that will allow them to create the theatrical kind of event they desire."[235]

Casualty Levels

- "Terrorists, therefore, are attracted to American interests and citizens abroad precisely because of the plethora of readily available targets; the symbolic value inherent in any blow struck against U.S. 'expansionism,' 'imperialism,' or 'economic exploitation,' and, not least, because of the unparalleled opportunities for exposure and publicity from perhaps the world's most extensive news media that any attack on an American target – especially on the involves civilian casualties – assures."[236]
- "The most obvious explanation for international terrorism's increasing lethality is that public attention is not as readily aroused as it was in the past. The general proliferation of terrorist movements and the consequent increase in terrorist incidents have created problems for both old and – especially – new groups who must now compete with others for a wider audience share. Terrorists have therefore been forced to undertake spectacular and bloody deeds in order to achieve the same effect a small action would have had ten your ago – and have apparently come to regard victims as an important ingredient of a successful attack."[237]

The Influence of Previous Attacks

- "'Avoid strength, and attack weakness'…asymmetric warfare…For Al Qaeda, this [idea] may be expressed in the succinct language of physical science as: *follow the path of least resistance*…resistance is adaptive learning. Al Qaeda is eager to learn from past terrorist experience – the successes and failures of attacks perpetrated by its own network, and by other terrorists around the world. Al Qaeda would tend to 'copycat' methods which either have proven to be successful, or are perceived to have the potential to be successful. If an attack mode has demonstrated effectiveness, or has the promise of being effective, it is likely to be an attack option."[238]

---

[233] McCormick, "Terrorist Decision Making," p. 484.
[234] Drake, *Terrorists' Target Selection*, pp. 10-11.
[235] McCormick, "Terrorist Decision Making," p. 480.
[236] Hoffmann, *Terrorist Targeting*, p. 17.
[237] *Ibid*, p. 3.
[238] Woo, "Understanding Terrorism Risk," p. 7.

- "[T]errorists consciously learn from one another."[239]
- "The more often an attack mode has been used, the more likely it is to be re-used in another terrorist operation."[240]
- "Agents overestimate their skills owing to attribution bias…Individuals ascribe their past failings to random events, but their successes to their skills. The consequence is that their projection of the space of eventualities will be rosy and they will underestimate the incidence of possible setbacks…People are unaware of their own track record and do not learn that their past projections were too optimistic and correct for it."[241]

Psychological Impact

- "The relationship between the physical target which is attacked and the psychological target which is affected is central to understanding why terrorists attack the targets which they do…violence is not necessarily aimed physically at the psychological target, but at making it behave in a particular way."[242]
- "The events of this past autumn [Fall 2001] demonstrated that terrorists could use *Bacillus anthracis* to incite fear and panic among the population and destabilize society's life without causing a large number of victims."[243]
- "[T]he real impact of terrorist attacks employing conventional tactics and weapons is often more psychological than real – both in terms of loss of life and destruction of infrastructure."[244]

Political Impact

- "Terrorism is actually a very deliberate and planned application of violence. In this respect, terrorism can be seen as a concatenation of five individual processes, designed to achieve sequentially, the following key objectives:
  1. Attention. Through dramatic, attention-riveting acts of violence, terrorists seek to focus attention on themselves and their causes through the publicity they receive, most often from news media coverage.
  2. Acknowledgement. Having attracted this attention, and thrust some otherwise previously ignored or hitherto forgotten cause onto the state's—or, often more desirably, the international community's—agenda, terrorists seek to parlay their new-found notoriety into winning acknowledgement (and perhaps even sympathy and support) of their cause.
  3. Recognition. Terrorists attempt to capitalize on the interest and acknowledgement their violent acts have generated by obtaining recognition of both their rights (e.g., acceptance of the justification of their cause) and of their particular organization as the spokesman of the constituency whom the terrorists purport to, or in some cases, actually do, represent.
  4. Authority. Armed with this recognition, terrorists seek the authority to effect the changes in government and/or society that is at the heart of their movement's struggle (e.g., change in

---

[239] Hoffman, "Modern Terrorist Mindset," p. 7.
[240] Woo, "Evolution of Risk Modeling," p. 6.
[241] Nassim Nicholas Taleb, "The Black Swan: Why don't we Lean that We Don't Learn?," draft of paper prepared for Highland Forum #23, January 2004, pp. 25-27.
[242] Drake, *Terrorists' Target Selection*, pp. 1-2.
[243] G. G. Onishchenko, "Bioterrorism as Threat to Biological Security: Assessment of Healthcare Institutions Preparedness to Counteract Bioterrorism," CEP 20030729000394 Moscow, citing *Vestnik Rossiyskoy Akdemii Meditsinskikh Nauk* 4 (April 2003), p. 9.
[244] Anderson, *Threat-Vulnerability Integration*, p. 4.

government or in the entire state structure, or the re-distribution of wealth, re-adjustment of geographical boundaries, assertion of minority rights, etc.).

5. Governance. Having acquired authority, terrorists seek to consolidate their direct and complete control over the state, their homeland and/or their people."

"Whilst some terrorist movements have been successful in achieving the first three objectives, rarely in modern times has any group attained the latter two. Nonetheless, all terrorists exist and function in hopes of reaching this ultimate end. For them, the future rather than the present defines their reality."[245]

Analysis:

A group's operational objectives are shaped by several factors, chief among which is the group's ideology. Important elements a group must consider, in addition to their primary purpose for carrying out a particular attack, are: desired casualty levels, level of publicity required, whether the target should be symbolic or whether an instrumental target suffices, the type and degree of reaction wanted from various audiences, expected secondary effects and reactions of the state and members of the terrorists' perceived constituency, and the scale of the attack. Competition with other groups can encourage greater attack scale. In terms of sustaining or building up the terrorist organization itself, large, successful attacks can boost morale and external support. It may well be that top-rung terrorist groups (such as Al-Qa`ida) have to keep pushing the envelope in terms of attacks to stay relevant and 'on top', whereas 'local' groups, so-called 'street terrorists' do not need to do spectaculars. In the context of unconventional weapons, they could be used not only as anti-personnel weapon, but also to contaminate and thus make certain facilities/infrastructure unusable, e.g. the psychological effects of RDDs.

15) Attack Modalities

There are a number of references in the literature to activities that fall broadly under the attack modalities rubric. Most fall into the general category, and only a few fall precisely within the various identified subfactors:

General

- "The first decision is political – determining appropriate and possible targets. Once a set of targets is decided on, they must be reconnoitered and information gathered on how to approach the targets, how to place the bomb, how the security of the individuals and the explosives need to be protected. Then the time is chosen and the specific target. Next there [is] a preliminary run-through – in our case a number of practice sessions…"[246] In short, determining the attack modality is generally a multi-step process.
- "A terrorist group's choices of targets, tactics, and timing represent its three degrees of freedom. It can choose what targets it will attack and when and how it will do so. Together, these choices define a group's 'operating profile.'"[247]
- "[K]nowledge, weapons, and information are necessary for a successful attack …"[248]
- "It is essential to understand weapons, tools, and tactics …"[249]
- "[T]errorists need to know whether [a target] is protected in order to gauge the degree of force needed to overcome any protective security…Reconnaissance is sometimes carried out by a separate terrorist unit to the one that actually carries out the attack."[250]

---

[245] Hoffman, "Modern Terrorist Mindset," pp. 16-17.
[246] Hoffman, "Modern Terrorist Mindset," p. 13, directly quoting a US left-wing radical who specialized in bombings.
[247] McCormick, "Terrorist Decision Making," p. 496.
[248] Ballard, *Preliminary Study of Sabotage and Terrorism*, p. 27.
[249] FEMA, *Reference Manual to Mitigate Potential Terrorist Attacks*, chapter 1, p. 14.

- "Following the path of least resistance in target selection means avoiding hard secure targets…Television publicity in the Middle East exposing U.S. defensive weaknesses simplifies and shortens the target search and surveillance process."[251]
- "…[M]ost, if not all, terrorist operations require a level of simplicity and cleverness as far from the maximum threshold of complexity as possible in order to achieve the desired outcome…This relationship between simplicity and success occurs because terrorist organizations, similar to military units in combat, become vulnerable to factors outside their sphere of control as soon as the mission enters its executions phase."[252]
- "[A]l-Qaeda terrorism activity…is [directed] towards the weapon modes and targets against which the technical, logistical and security barriers to mission success are least."[253]
- "Attributes of the attack means which must be considered include:
    1. Accuracy – degree of difficulty in delivering the attack means to the target
    2. Destructive Capacity – payload size, weight, speed
    3. Flexibility – degree of difficulty in attack coordination and presence of contingency plans
    4. Opportunity – access to the target"[254]

Choice of Weapons

- "The most significant conventional attacks that produced mass casualties and mass destruction in the 1990s…all, unfortunately, demonstrated the ease with which terrorists can procure the necessary materials, fashion them into powerful weapons, and deliver them to targets."[255]

Insiders and Outsiders

- "Adversaries have different levels of access…Insiders might be less likely to attack a system than outsiders are, but systems are far more vulnerable to them…An insider knows how the systems work and where the weak points are. He knows the organizational structure, and how any investigation against his actions would be conducted. He may already be trusted by the system he is going to attack. An insider can use the system's own resources against itself. In extreme cases the insider might have considerable expertise, especially if he was involved in the design of the systems he is now attacking."[256]

Analysis:

Depending upon the nature of that target, particular weapons and tactical approaches will be chosen that seem most likely to enable the terrorists to a) carry out a successful attack and thence, except in the case of suicide bombers, b) escape without being killed or apprehended. In short, *the nature of the target itself is the most decisive factor in determining the choice of modalities used to attack it, although the range of those modalities is also limited to some extent by the existing capabilities of the group*.

E. Conclusion

---

[250] Drake, *Terrorists' Target Selection*, pp. 61-62.
[251] Woo, "The al-Qaeda War Game," p. 1.
[252] Palfy, "Weapon System Selection," p. 87.
[253] *Ibid*, p. 1.
[254] Anderson, *Threat-Vulnerability Integration*, p. 5.
[255] Parachini, "Comparing Motives and Outcomes of Mass Casualty Terrorism," p. 391.
[256] Schneier, *Secrets and Lies*, pp. 42, 48.

Given that the literature sample examined was restricted to general treatises on terrorism, and did not include studies of particular terrorist groups, we believe that there is much of value to be found in what is an admittedly preliminary analysis of influences on terrorist motivations to attack CI. The following chapter attempts to inform this analysis which illustrates historical examples of terrorist attacks against CI.

Chapter 3: HISTORICAL RECORD AND SELECTED CASE STUDIES*

A. Introduction

The importance of carrying out in-depth *qualitative* research as part of any serious effort to assess the motivations of terrorists, whether for attacking Critical Infrastructure (CI) or other sorts of targets, cannot be overemphasized. In addition to attempting to discern terrorist motivations for attacking CI by adopting a *macro-viewpoint*, which among other approaches may involve consulting the existing secondary literature to determine the consensus of scholars working in the field and/or creating models to weigh the various factors that seem to indicate the proclivities of terrorists, a thorough analysis is incomplete without a *micro-approach* based on the careful examination of what "really-existing" terrorist groups have actually done. It is only after examining the actions taken by diverse terrorist groups in considerable detail that one can hope to draw general conclusions that have a firm basis in reality.

Due to temporal constraints the project team was compelled to limit the depths of this approach in its efforts to shed light on past and present terrorist motivations for attacking CI. Nonetheless, the project team selected case studies that were assessed to highlight as many salient points as possible. The procedure adopted below is first to discuss general historical patterns of terrorist attacks on CI, focusing both on the types of groups that have made such attacks and on the types of targets they have attacked. In order to illustrate these general patterns, we then provide several case studies which were selected, not so much because they were considered "representative" as because they served to illustrate certain problems and/or illuminate important factors in the analysis of terrorist motivations for attacking CI. On the basis of this combination of a general analysis of past terrorist attacks on CI and case studies, together with additional information that can be gleaned about more recent patterns of terrorism and threats to CI, the conclusion to this chapter offers a preliminary assessment of likely present and future threats.

B. Historical Patterns of Terrorist Attacks on CI

If one hopes to be able to forecast potential future terrorist attacks on CI with any degree of accuracy, it is first necessary to obtain a better understanding of why such groups have previously opted to attack CI. In this section an analysis of general patterns of prior subnational attacks on CI will be followed by a few select case studies of groups that consciously chose to attack infrastructural targets.

General Patterns of Non-State Actor Attacks on CI

To shed further light on why certain types of terrorist groups might be more inclined to carry out CI attacks than others, it is probably most useful to divide the post-World War II history of terrorism into 1) an earlier era dominated by secular (or at least secularized) political terrorist organizations demanding political independence or espousing utopian revolutionary ideologies, whether of the left or right; and 2) a more recent period in which religious terrorism, i.e., terrorism inspired by religious doctrines and imperatives, has come to the fore.[257]

---

* This chapter was written by Jeffrey M. Bale, except for the section on Chukaku-Ha, which was written by Kevin S. Moran; the section on the Indian Parliament Attack, which was written by Sundara Vadlamudi; the section on Radical Ecology Groups, which was written by Gary Ackerman and Kevin S. Moran; and the Tentative Conclusions section, which was written by Kevin S. Moran and Sundara Vadlamudi.

[257] Cf. Bruce Hoffman, *Inside Terrorism* (New York: Columbia University, 1998), pp. 87-95.

During this latter period, "a surge of religious fanaticism has manifested itself in spectacular acts of terrorism all across the globe…[a] wave of violence that is unprecedented, not only in its scope and the selection of targets, but also in its lethality and indiscriminate character."[258] It may well be that the factors affecting decisions to attack CI differed somewhat, and in certain respects perhaps quite significantly, during these two eras.

As noted earlier, the first of these two periods, which lasted roughly from the mid-1960s to the early 1980s, was dominated on the one hand by nationalist/separatist/irredentist terrorism and on the other by ideological left and right-wing terrorism. One would therefore expect to find that terrorist groups within those categories had carried out more attacks against CI than the relatively few and insignificant groups of violent religious extremists during that era. One could also predict that as religious terrorism resumed its importance from the mid-1980s to the present day, the proportion of CI attacks carried out by religious terrorists would also rise. Indeed, when one examines the descriptive statistics concerning the number of CI attacks carried out by different types of terrorist groups (see Chapter 4), these suppositions turn out to be quite correct.

Case Study Illustrating the Methodological Problems Involved in Categorizing Terrorist Attacks as Attacks on CI

Before turning to three case studies in which particular terrorist groups specifically targeted CI, an example should be provided that serves to illustrate the methodological problems involved in categorizing terrorist attacks as infrastructural in the first place. In theory, key government facilities clearly fall into the category of CI, but in reality most of the attacks launched against such facilities, including overseas embassies, are not primarily intended to disrupt their functioning. On the contrary, terrorists generally have multiple motives for attacking such targets (e.g., the Murrah Federal Building in Oklahoma City or the World Trade Center), the *least* of which is to interfere with the operation of a country's vital infrastructure. Although this may well be *one* of their reasons for launching attacks of this sort, their principal motive is normally either to attack a high-profile symbolic target so as to traumatize a country's populace psychologically, or simply to kill large numbers of people, perhaps especially government officials. The following case, the December 2001 attack by Kashmiri Islamists on the Indian Parliament, is an excellent example which perfectly underscores the problems involved with identifying particular attacks as infrastructural in the narrowest sense of that term.

The Indian Parliament Attack

On 13 December 2001, suspected members of the Jaish-e-Mohammed (JEM: Army of Muhammad) militants attacked the Indian Parliament, killing 9 people before being gunned down by security personnel guarding the building. The attack could be construed as an attack against CI since the legislative body in India is instrumental in ensuring the Continuity of Government (CoG). The attack on the Indian Parliament, as outlined in the following sections, was aimed at wiping out the Indian political leadership and delivering a message of strength and resolve by attacking a symbolic target.

---

[258] Magnus Ranstorp, "Terrorism in the Name of Religion," in *Terrorism and Counterterrorism: Understanding the New Security Environment*, ed. by Russell D. Howard and Reid L. Sawyer (Guilford, CT: McGraw-Hill, 2002), p. 122. This article originally appeared in the Summer 1996 issue of the *Journal of International Affairs*. Of course, as David Rapoport and many others have pointed out, religious motivations had long served as the primary inspiration for terrorism, and in that sense their recent flowering in virulent new guises is only surprising insofar as they have partially displaced secular motivations that were once thought to signal the decline of religiosity. Alas, since the mid-1970s there has been an unanticipated resurgence of religiosity in many parts of the world. See, e.g., Gilles Kepel, *The Revenge of God: The Resurgence of Islam, Christianity and Judaism in the Modern World* (University Park: Pennsylvania State University, 1994).

The following sections will discuss the general characteristics of the JEM, the details of the attack on the Indian Parliament, and present some conclusions discussing the challenges posed by attacks against CI targets that are not primarily aimed at interfering with the socio-economic activities of the population. Two points need to be clarified prior to summarizing the attack on the Indian Parliament. The first is the identity of the terrorist group involved in the attack. In the initial days following the attack, India blamed the militant group Lashkar-e-Tayyiba (LET: Army of the Righteous) for orchestrating the attack. India's Minister for External Affairs Jaswant Singh said that "there is credible technical evidence that yesterday's terrorist attack … was the handiwork of terrorist organization lashkar-e-toyeba (sic)."[259] The LET, however, denied the charges.[260] Both the U.S. State Department and the Indian Deputy Prime Minister L.K. Advani in a statement in the Indian Parliament after the attack indicated that the attack was carried out by the JEM and the LET.[261] However, as will be outlined below, the attack was carried out by JEM members and the LET only provided some logistical support for the operation. Hence, only the characteristics of the JEM will be detailed herein.

Second, some confusion still exists about the precise number of attackers. News reports have claimed the size of the attack team to be between five and seven.[262] The official statement issued by the Home Minister L.K. Advani indicates that 5 persons attacked the Parliament, and this figure will be used as the basis for our analysis.

Group Characteristics – Jaish-e-Mohammed (JEM). Jaish-e-Mohammed is an Islamist militant group based in Pakistan. The JEM was formed by Maulana Masood Azhar between January and March 2000 following his release from Indian custody on December 31, 1999 in exchange for 155 hostages in the hijacking of Indian Airlines Flight IC 814. The group has mainly carried out attacks in Jammu & Kashmir, the sole exception being the attack on the Indian Parliament. The JEM was included in both the US Treasury Department's Office of Foreign Asset Control (OFAC) list in October 2001 and the US State Department Foreign Terrorist Organizations list in December 2001, and it has since been renamed Khuddam-ul-Islam. At the time of the attack, however, the group was still known as JEM.[263]

JEM advocates a violent struggle to liberate Kashmir from India. Apart from liberating Kashmir, JEM also propagates a pan-Islamic agenda aimed at liberating Muslims world-wide. Prior to the attack on the Indian Parliament, JEM carried out an attack on the Kashmir State Assembly in October 2001, killing 38 people. The plan of attack on the Indian Parliament was similar to the attack on the Kashmir State Assembly. JEM claimed responsibility for the attack on the Kashmir State Assembly but retracted that claim the next day. However, the group did not claim responsibility for the attack on the Indian Parliament.

A clear picture of the group's organizational structure is difficult to portray owing to the secretive nature of the group and the constant changes in its hierarchy. Maulana Masood Azhar is the *Amir* and the founder of the JEM.

---

[259] "India Blames Pakistan-based Militant Groups for Attack on Parliament," Deutsche Presse-Agentur, December 14, 2001.
[260] "LeT denies Involvement in Attack on Indian Parliament," Press Trust of India, December 14, 2001.
[261] "Appendix A: Chronology of Significant Terrorist Incidents, 2001," *Patterns of Global Terrorism*, U.S. Department of State, http://www.state.gov/s/ct/rls/pgtrpt/2001/html/10252.htm (Accessed on July 21, 2004); "India Accuses Pakistan of Involvement in Terrorist Attack on Parliament," BBC Monitoring South Asia, December 18, 2001.
[262] "Seven in Suicide Attack, not Five," *The Statesman* (India), December 15, 2001; "Confusion Over Presence of a Sixth Terrorist," Press Trust of India, 13 December 2001; "Numbers Mystery," *The Statesman* (India), December 17, 2001.
[263] "Jaish-e-Mohammed (JEM) (Army of Mohammed), Appendix B: Background Information on Designated Foreign Terrorist Organizations," *Patterns of Global Terrorism 2001*, U.S. Department of State, http://www.state.gov/s/ct/rls/pgtrpt/2001/html/10252.htm#jem (Accessed on July 21, 2004); "Jaish-e-Mohammad Mujahideen E-Tanzeem," South Asia Terrorism Portal (Internet Site), http://www.satp.org.

The following description is an attempt to shed at least some light on the group's structure.

- Maulana Masood Azhar – Founder and Amir (Commander)
- Maulana Muhammed Yousuf Ludhianvi – Co-Founder (killed in May 2000)
- Maulana Nizamuddin Shamzai – Co-Founder (killed in May 2004)
- Maulana Abdul Jabbar – *Nazim*, Military Affairs (was banned from JEM, then formed a splinter group called Jamaat-ul-Furqan)
- Maulana Sajjid Usman – Finance Chief
- Maulana Qari Mansoor Ahmed – *Nazim*, Propaganda

Other organizational posts indicate an organizational structure with regional branches in Pakistan occupied Kashmir (POK), Jammu & Kashmir, Punjab, and Karachi.[264]

The State Department's *Patterns of Global Terrorism 2003* estimates the JEM's cadre strength at several hundred armed men.[265] The actual number may be several times as great. The group's members reportedly comprise Pakistanis and Kashmiris, as well as Afghans and Arabs who fought in the Afghan war during the 1980s.[266]

JEM has renamed itself several times to avoid official sanctions. Immediately following the attack on the Kashmir State Assembly, JEM was renamed Tehrik ul-Furqaah to avoid the repercussions of its inclusion on the US list of Foreign Terrorist Organizations.[267] JEM was renamed as Khuddam ul-Islam in March 2003.[268] In July 2003, JEM splintered. The breakaway group, led by Maulana Abdul Jabbar, formed the Jamaat ul-Fuqran.[269]

JEM adheres to the Sunni Deobandi ideology, and as a result the role of women in the organization can be assumed to be limited if not non-existent. JEM's attacks have not involved women, and information on the role of women in other organizational activities is largely non-existent. JEM recruits most of its members from the Madrassahs (Islamic seminaries) in Pakistan. The organization's senior positions are held either by veterans of the Afghan conflict or by senior Islamic *mullahs*. JEM members are believed to be proficient in the use of light and heavy machineguns, assault rifles, mortars, improvised explosive devices, and rocket-propelled grenades.[270]

JEM was the first militant group to introduce suicide attacks in Kashmir.[271] Ever since it initiated the Fidayeen (suicide attack) tactic in Kashmir in April 2000, an average of one suicide attack per month has occurred in the state.[272] JEM had a large training camp in the North-West Frontier Province capable of handling between 800 – 1,000 volunteers,[273] and it also operated training camps in Afghanistan until the American-led invasion of Afghanistan in 2001.[274]

---

[264] "Jaish-e-Mohammad Mujahideen E-Tanzeem," South Asia Terrorism Portal (Website); K. Santhanam et. al., *Jihadis in Jammu and Kashmir: A Portrait Gallery*, (New Delhi, London: SAGE Publications, 2003), pp. 196-197.
[265] "Jaish-e-Mohammed (JEM) (Army of Mohammed) a.k.a. Tehrik ul-Furqaah, Khuddam-ul-Islam,
Appendix B: Background Information on Designated Foreign Terrorist Organizations," *Patterns of Global Terrorism 2003*, U.S. Department of State, http://www.state.gov/s/ct/rls/pgtrpt/2003/31711.htm (Accessed July 21, 2004).
[266] Ibid.
[267] "Jaish-e-Mohammed adopts new name," *Rediff* (Internet Site), http://www.rediff.com/us/2001/oct/11ny24.htm (Accessed July 23, 2004).
[268] "Jaish, Harkat Change Names: Report," *Rediff* (Internet Site), http://www.rediff.com/news/2003/mar/12pak.htm?zcc=rl. (Accessed July 23, 2004).
[269] *South Asia Intelligence Review: Weekly Assessments & Briefings*, Vol. 1, No. 51 (July 7, 2003).
[270] "Jaish-e-Mohammed (JEM), Appendix B," *Patterns of Global Terrorism 2003.*
[271] K. Santhanam et. al., *Jihadis in Jammu and Kashmir*, p. 201.
[272] Praveen Swami, "Profile of a Terror Outfit," *Frontline*, Vol. 18, No. 26 (December 22, 2001 – January 04, 2002).
[273] K. Santhanam et. al., *Jihadis in Jammu and Kashmir*, p. 200.
[274] "Jaish-e-Mohammed (JEM), Appendix B," *Patterns of Global Terrorism 2003*.

JEM is well connected to the religious political parties in Pakistan, Islamic organizations, the Taliban, al-Qa`ida, Sunni sectarian groups in Pakistan, and other militant organizations fighting Indian security forces in Indian-administered Kashmir. JEM's foundation was supported by Mufti Nizamuddin Shamzai of the Majlis-e-Tawan-e-Islami (MT), Maulana Mufti Rashid Ahmed of the Dar-ul Ifta-e-wal-Irshad and Maulana Sher Ali of the Sheikh-ul-Hadith Dar-ul Haqqania. Among the Islamic political parties, it is associated with the Jamiat Ulema-e-Islam Fazlur Rahman faction (JUI-F). JEM is also believed to possess links to the Sunni sectarian groups Sipah-e-Sahaba Pakistan (SSP: Soldiers of the Companions of the Prophet Muhammad) and the Lashkar-e-Jhangvi (LJ: Army of Jhangvi). It shares resources with other militant groups operating in Kashmir such as Harkat ul-Jihad-i-Islami (HUJI: Islamic Jihad Movement), Harkat ul-Mujahideen (HUM: Movement of Holy Warriors), and LET.[275]

JEM's supporters are mainly Pakistanis and Kashmiris, with its support base located primarily in Pakistan, Pakistan-administered Kashmir, the Doda district in Kashmir, and the southern parts of Kashmir. JEM draws a large number of supporters from the madrassahs in Pakistan. Like other terrorist groups operating in Kashmir, JEM can be considered to be generally familiar with the population in the region.

JEM is suspected of receiving support from Pakistan's intelligence service, the Inter Services Intelligence (ISI) agency. Indian authorities have claimed that Pakistan's ISI recruits, trains, and sends militants across the border to conduct terrorist attacks in Indian-administered Kashmir, but Pakistani authorities deny the charges.[276] JEM, like other militant groups fighting in Kashmir, enjoys widespread support among the Islamic parties and militant groups in Pakistan, certain sections of the Pakistani government, and some percentage of the population in Indian-administered Kashmir. Even though specific information on JEM's collaboration with criminal groups is not readily available, such a possibility cannot be ruled out, since Pakistan's sectarian extremist groups and drug traffickers have helped one another to advance their respective interests.

Physical Characteristics of the Indian Parliament. The Indian Parliament estate covers about 6 acres and has 3 layers of security. The attackers were able to breach the first layer of security, but were killed before they could penetrate the next two layers. The 3-tiered security system consists of about 1,250 personnel drawn from the Delhi Police (200), the Central Reserve Police Force (850), and the Parliament's unarmed Ward and Watch (W&W) staff.[277]

Planning and Execution. The attack was carried out by five JEM militants code-named "Mohammad", "Rana", "Raja", "Tufail", and "Hamza". The group was led by "Mohammad". The collaborators in the scheme were Shaukat Ahmad Ansari, Ansari's cousin Mohammad Afzal Ansari, and Syed Abdul Rahman Jeelani, a lecturer at the Zakir Hussain College in New Delhi. Mohammad Afzal Ansari, a former member of the Jammu and Kashmir Liberation Front (JKLF), a militant organization fighting for Kashmir's independence, became involved in the conspiracy in mid-February 2001, when he was ordered by JEM's operations chief in Kashmir, Ghazi Baba, to set up a base in New Delhi to facilitate the organization's activities. The five-member team was dispatched to India in mid-2000 to identify potential targets for attack. Mohammad Tariq, Ghazi Baba's deputy, was ordered to liaise with the team. For reasons unknown to Indian intelligence officials, "Mohammad", the team's leader, is believed to have decided to attack targets in New Delhi. He arrived in New Delhi in mid-November (according to some reports, October), whereas other members of the team followed later. The Ansari cousins and Jeelani provided assistance by locating housing and helping to set up the base in New Delhi. The Ansari cousins also assisted in transporting the cell members and their arms from Kashmir.

---

[275] "Jaish-e-Mohammad Mujahideen E-Tanzeem," South Asia Terrorism Portal; "Jaish-e-Mohammed (JEM), Appendix B," *Patterns of Global Terrorism 2003*.

[276] "In the Spotlight: Jaish-e-Mohammed (JEM)," Center for Defense Information (CDI) Terrorism Project http://www.cdi.org/terrorism/jem-pr.cfm (Accessed July 21, 2004).

[277] Sayantan Chakravarthy et all, "The Day India was Targeted," *India Today*, December 24, 2001.

The arms used in the attack were brought from Kashmir and included 4 AK-47 rifles, 3 pistols, 12 magazines, 1 grenade-launcher, 15 shells, 15 hand-grenades, 2 packets of detonators, radio-activated devices, and 2 wireless sets. However, materials like ammonium nitrate, sulfur, and aluminum, which were needed for building explosives, were bought in New Delhi. Indian investigators believe that the arms were acquired and supplied by Lashkar-e-Tayyiba. The agreement on cooperation, though unconfirmed, is believed to have been finalized between JEM's Amir Masood Azhar and LET's overall operations commander Zaki-ur-Rehman. Investigators believe that the group decided to attack the Parliament instead of the Indira Gandhi International Airport because the Parliament afforded better chances of penetration with a car resembling a government-owned vehicle. Indian investigators also believe that the finances for the operation were coordinated by contacting hawala operators in Germany.[278]

JEM has used suicide attacks to cause the maximum negative impact on the security situation in Kashmir. In a typical fidayeen attack, JEM militants would storm the target and then fortify themselves inside it. After the members gain entry to the target, JEM members attempt to kill as many security personnel or civilians as possible before they are killed themselves. In some instances, the attackers caused maximum damage and then managed to escape from the security forces.[279]

Five members of the JEM entered the premises of the Indian Parliament by posing as security escorts to a parliamentarian. The attackers used a white Ambassador car (commonly used by the security agencies) with a flashing beacon and a sticker identifying the vehicle as belonging to the Home Ministry. The car was packed with 30 kg of RDX, possibly for causing an enormous explosion to gain entry into the building. After breaching the first layer of security, the car accidentally hit one of the escort vehicles of the Vice-President, upon which a security escort for the Vice-President engaged the attackers. The attackers got out of the car and began firing indiscriminately while lobbing grenades at the security personnel. The Parliamentary security personnel, watching the unfolding commotion, immediately ordered the entry gates to the Parliament to be closed, thereby blocking the attackers' entry into the main building. The attackers targeted 3 different gates of the building, but all 5 militants were killed by security personnel before they could reach the gates.[280]

The attackers gathered information regarding the target by conducting surveillance of the Parliament building and taking pictures of the building using a digital camera. These pictures were later fed into a laptop computer to generate a visual topography of the building. Hand-drawn maps were also used to plan the attack. A Parliamentary Staff member was arrested for passing important documents to a Pakistani embassy official and during the investigation the staff member revealed that this Pakistani embassy official had enquired about the security arrangements at the Parliament. The role of the Pakistani embassy official in the attack still remains unclear.[281]

---

[278] "India: Investigators Crack Contours of Parliament Attack," *Businessline*, December 17, 2001; in Proquest, ProQuest Document ID: 95558303, December 17, 2001, http://proquest.umi.com; "Mohammad Afzal: Candid Canary," *India Today*, December 31, 2001; Praveen Swami, "On the Terrorist Trail," *Frontline*, Vol. 18, No. 26, (December 22, 2001-4 January 2002); "JeM Carried out Parliament Attack with ISI Guidance," Press Trust of India, December 16, 2001; "Following is the Chronology of Events Leading to the Attack on Indian Parliament on December 13," December 16, 2001.

[279] "Jaish-e-Mohammad Mujahideen E-Tanzeem," South Asia Terrorism Portal, http://www.satp.org.

[280] "Suicide Attack on Parliament, Six Securitymen among 12 Killed," The Press Trust of India, December13, 2001; Nirmala George, "Terrorist Attack on Indian Parliament leaves 12 Confirmed Dead," The Associated Press, December 13, 2001; "A Minute-by-Minute Account," *The Hindu* (India), December 14, 2001.

[281] "Militants Posed as Tourists to Take Snaps of Parliament," Press Trust of India, December 23, 2001. "Laptop was Used by Terrorists to Generate Map of Parliament," Press Trust of India, December 19, 2001. "Police Probing Link Between Dec 13 Attack and PHC Staffer," Press Trust of India, December 24, 2001, Harbaksh Singh Nanda, "India Expels Pakistani Embassy Staffer," United Press International, December 24, 2001.

Conclusions. The attack on the Indian Parliament is indicative of the difficulties commonly facing analysts who are attempting to study terrorist motivations for attacking CI. Most of the attacks on critical infrastructure are not solely aimed to disrupt or destroy the functioning of the vital infrastructures needed to ensure the supply of socio-economic goods and services to the nation. Most often, attacks against high profile targets have several purposes other than disruption, destruction, and distraction. The attack on CI might also serve as a symbolic attack. The attackers of the Indian Parliament planned to kill as many Members of Parliament (MPs) as possible. Afzal Ansari, one of the collaborators for the attack, informed the investigators that "Mohammed" was instructed to cause maximum killing inside the Parliament.[282] Indian investigators have also speculated that the terrorists planned to take some hostages, a fact borne out by the presence of dry fruits and rope among the terrorists' possessions.[283] According to an Indian intelligence officer, the terrorists' use of cell phones until the very end could be explained by their intention to use them during the hostage negotiations.[284]

Any outcome would have severely affected the ability of the Indian Parliament to conduct its essential legislative tasks. The attack on the Parliament had an immediate effect on the nation's stock markets. The Bombay Stock Exchange (BSE) suffered an intra-day loss of 132 points immediately after the news of the attack broke out. However, the stock market recovered later in the day and suffered a net loss of only 23 points over the previous day. The Indian rupee fell by about 6 paise against the US Dollar.[285] It is highly unlikely that the dominant motive for the attack was to disrupt the legislative process. The attack had more to do with the symbolic nature of the Indian Parliament than its legislative function. However, the ripple effects of the attack caused minor disruptions in the economic markets and the attack, if it had succeeded, would have severely disrupted the functioning of the country. The Indian Prime Minister Atal Behari Vajpayee rightfully observed that "[the] Parliament House was selected in a well thought-out plan because the terrorists also understand that the parliament is the heart of the Indian Republic, which also represents the whole country and is the axis of the national unity."[286]

The case of the attack on the Indian Parliament indicates that, when assessing attacks against CI targets, all possible motives need to be considered, not just those specifically aimed at disrupting or crippling the functioning of the nation's infrastructure.

Case Studies of Terrorist Groups that have Focused on Attacking CI

In order to flesh out the basic statistical picture painted by the CrITIC Database and discussed in Chapter 4, a few examples of specific terrorist groups that have previously focused on CI targets should be briefly discussed. This may help to provide some indications of various motives for focusing on CI, which may then assist analysts in determining what types of groups may carry out future attacks of this sort.

---

[282] "Militants had Instructions to Mow down MPs," Press Trust of India, December 20, 2001.
[283] "Were Terrorists Planning a Prolonged Stay," The Press Trust of India, December 13, 2001; in Lexis-Nexis Academic Universe, December 13, 2001, http://web.lexis-nexis.com.
[284] Celia W. Dugger, "India says Arrests Link Militants in Pakistan to Attack," *The New York Times*, December 17, 2001; in Lexis-Nexis Academic Universe, December 17, 2001, http://web.lexis-nexis.com.
[285] "Sensex Down on Bombay Stock Exchange," Xinhua General News Service, December 13, 2001; in Lexis-Nexis Academic Universe, December 14, 2001, http://web.lexis-nexis.com; "India: Stocks Shiver but Recover," *Business Line*, December 14, 2001; in Lexis-Nexis Academic Universe, December 14, 2001, http://web.lexis-nexis.com.
[286] "Indian Prime Minister Advocates Diplomacy First in Wake of Attack on Parliament," BBC Monitoring South Asia-Political, December 19, 2001.

Fronte di Liberazione Naziunale di a Corsica/Front de Libération Nationale de la Corse (FLNC)

The FLNC is one of several nationalist/separatist groups that have frequently attacked CI targets, along with ETA, the LTTE, and the IRA. Given the peculiarities of the Corsican context, this is entirely understandable. Yet one must bear in mind that those very peculiarities may mean that the FLNC's motives for attacking CI are neither easily generalized nor entirely applicable to other groups.

Corsica is an island in the Mediterranean Sea that lies off the western coast of Italy, but since 1768 it has essentially been administered directly by France as a province. The contemporary nationalist struggle in Corsica dates back to the mid-1950s, and was fueled by a combination of general economic underdevelopment and discriminatory French policies that encouraged citizens from both the mainland and France's former North African colonies to settle and buy land and property on the island, on whose coasts French officials hoped to establish a thriving tourist industry. As a result both land and jobs often went to outsiders at the expense of Corsicans, many of whom were forced to emigrate to France or other countries in order to make a decent living. The islanders naturally resented the influx of favored and wealthy foreigners, and increasingly came to the conclusion that France was treating their homeland as an internal colonial possession.[287] Their resistance initially took the form of political action and peaceful protests, but when these failed to achieve desired results a more assertive nationalist movement emerged whose radical fringes took up armed struggle against the French state beginning in the mid-1970s. In August 1975, the spark was ignited by a violent confrontation on a settler-owned vineyard in Aléria between a few armed occupiers from the Action Régionaliste Corse (ARC: Corsican Regional Action), then the primary nationalist political organization, and 1,200 riot police from the island's Compagnies Républicaines de Sécurité (CRS: Republican Security Companies). This incident, which resulted in three deaths, was soon followed by the arrest of ARC leaders and the banning of their organization, a move that convinced several exasperated nationalists that violence had become necessary to achieve their goals.[288] Henceforth the Corsican nationalist struggle was waged on two fronts: 1) legal political action by the successors of the ARC – above all the Union diu Populu Corsu (UPC: Corsican People's Union) – in favor of cultural determination and autonomy, and 2) clandestine armed struggle by militant groups promoting "national liberation," i.e., secession from France and independence. In May 1976 elements of three earlier armed groups, the ARC's commandos, the Fronte Paisanu Corsu di Liberazione (FPLC: Corsican Peasant Liberation Front or Native Corsican Liberation Front), and Ghjustizia Paolina (GP: Paoline Justice), coalesced into a new clandestine group, the FLNC.[289]

The ideological agenda of the FLNC was made clear in its founding document, the "Manifeste du 5 mai [1976]," which presented a program with the following goals: 1) recognition of the national rights of the Corsican people; 2) removal of all the instruments of French colonialism, including the army, administration, and French colonists; 3) establishment of a popular democratic government that will express the interests of all Corsican patriots; 4) the carrying out of agrarian reform to fulfill the aspirations of peasants, workers, and intellectuals, as well as rid the country of all forms of exploitation; and 5) ensuring the right of self-determination for the Corsican people

---

[287] For a brief history of Corsica, see Paul Arrighi and Francis Pomponi, *Histoire de la Corse* (Paris: Presses Universitaires de France, 1978). For the general postwar context within which contemporary Corsican nationalism emerged, see Xavier Crettiez, *La question corse* (Paris: Complexe, 1999), pp. 17-86; and Robert Ramsay, *The Corsican Time-Bomb* (Manchester: Manchester University, 1983), pp. 31-95.

[288] For this "Aléria incident" and its impact, see Ramsay, *Corsican Time-Bomb*, pp. 99-104; and the partisan account of ARC leader Edmond Simeoni, *Le piège d'Aléria:Les raisons de la colère des Corses* (Paris: J. C. Lattès, 1976).

[289] For the creation of the FLNC, see especially the inside account of FLNC leader Jean-Pierre Santini, *Front de Libération Nationale de la Corse: De l'ombre à la lumière* (Paris: L'Harmattan, 2000), pp. 7-37. Cf. Ramsay, *Corsican Time-Bomb*, pp. 118-19. The Paolina in the GP's name is a reference to Corsican nationalist and constitutional theorist Pasquale Paoli (1725-1807), the so-called "Father of the Corsican Nation." For more on Paoli, an Enlightenment figure who also influenced American constitutional development, see Antoine-Marie Graziani, *Pascal Paoli: Père de la patrie corse* (Paris: Tallandier, 2002).

after a three-year transitional period.[290] However, the basic underlying aim of the FLNC had earlier been revealed in a May 1975 document prepared by the left-leaning Partitu di u Populu Corsu (PCS: Corsican People's Party), the group to which Jean-Pierre Santini belonged before becoming a leader of the FLNC: to wage a "struggle for national liberation" and "self-determination" against the "capitalist and colonialist French state."[291] However, there were two distinctive features of the FLNC's ideology that serve to distinguish it from those of many other nationalist movements. First of all, the FLNC always refused to provide an explicitly revolutionary justification for its clandestine violence, and instead developed a "non-revolutionary nationalism" based upon the defense of the Corsican homeland and the "historic rights of the Corsican people." This lack of revolutionary pretensions, despite the FLNC's belated 1989 advocacy of an "original socialism" rooted in traditional Corsican communalism, in part explains why the group never waged a total assault on the forces of order or the French state.[292] Second, the nationalist doctrines of the FLNC and its predecessors were from the very outset infused with ecological concerns, and indeed the first act of nationalist terrorism was carried out on September 14, 1973 against the very same Italian vessel owned by Montedison that had earlier been responsible for polluting the Bay of Bastia (in the so-called "Red Mud" affair). The FLNC's popular "green" concerns were made explicit in its 1984 "white book," whose authors denounced "ecological aggression" and asserted (with considerable justification) that "only our political-military presence has impeded the almost total spoliation of our land by major European capitalist interests."[293] This also helps to explain why the tourist industry was so frequently targeted by the FLNC.

On paper the FLNC's organization appears to be a pyramidal, hierarchical structure in which orders are passed from a leadership directorate on down to local units. At the top lies the Cunsigliu or Council, a body of between 4 and 15 persons who are in theory responsible for coordinating the group's political and military action. This Council is in turn divided into four functional commissions, one concerned with military and logistical affairs, one with financial and economic affairs, one with managing the organization's "counter-power" apparatus (i.e., its front groups and linkages to legal nationalist parties), and the last with international propaganda activities. Under these bodies are six regional groups located in Bastia, Balagne, Corte, the Eastern Plain, Ajaccio, and Porto Vecchio, each of which have subsections. Within these subsections, which are also organized on a geographical basis, are the actual operational cells, 3-man groups which organize and carry out attacks.[294] However, this diagram is misleading insofar as it suggests that the directorate exercised top-down control over the sections, subsections, and cells, which in fact have always operated more or less independently. Indeed, the reality is that the FLNC has never been a monolithic organization, but rather a collection of autonomous localized cellular groups whose members have generally been well-integrated into their local communities. Furthermore, factionalism has been common on all levels, so much so that it generated severe tensions and periodically precipitated outright organizational schisms and the subsequent creation of new groups. For example, in 1987 Gravone sector leader Jean-André Orsini and two others broke away from the parent body and created a separate "parallel FLNC," and in 1988 local groups in Balagne and Marana-Bastia established a new clandestine nationalist group known as the FLNC – Canal Historique (FLNC – Historic Channel) in opposition to the main organization, which in 1990 renamed itself the FLNC – Canal Habituel (FLNC – Customary

---

[290] Note that there is an important discrepancy between the citations from this document in Santini, *Front de Libération de la Corse*, pp. 30-1; and Ramsay, *Corsican Time-Bomb*, pp. 118-19. The latter lists an additional and rather radical goal of the FLNC program – "[t]he confiscation of colonial estates and the property of tourist industry trusts" – which is omitted by the former. Yet Santini includes the rest of the manifesto, including the portion that enumerates the various crimes allegedly attributable to "French colonialism" in Corsica, above all the "destruction of our identity with the help of local elites."

[291] Santini, *Front de Libération de la Corse*, pp. 9-10, citing the document "Vers la Libération Nationale de la Corse."

[292] Crettiez, *Question corse*, pp. 159-61. Utopian forms of socialism, including Marxism, were apparently not very popular in Corsica.

[293] *Ibid*, pp. 163-5.

[294] Compare *ibid*, p. 116; and Jean-Michel Rossi and François Santoni, *Pour solde de tout compte: Les nationalistes corses parlent* (Paris: Denoël, 2000), Appendix 1, p. 227 (from the reproduction of a classified Gendarmerie Nationale report dated July 13, 1988.

Channel). The FLNC – Canal Historique later gave birth to still other factions, such as the Fronte Ribellu (Rebel Front), whereas the FLNC – Canal Habituel resumed the name FLNC in 2000. In the meantime, groups of young toughs who were attracted by the group's "cult of clandestinity" but lacked their predecessors' ideological commitment had emerged, which only accelerated the process of gradual FLNC atomization and criminalization.[295] These particular organizational factors had two contradictory effects on the level of FLNC violence. On the one hand, the immersion of FLNC cell members (who were often simultaneously members of legal nationalist parties) within their local communities generally acted as a brake on their employment of lethal or indiscriminate violence. On the other, the above-noted process of factionalization often resulted in temporary increases in acts of lethal violence, since the newly-emerging groups wished to establish their credentials by demonstrating their courage and operational effectiveness.[296]

Like most other non-state actors who resort to violence, the FLNC has tended to carry out attacks on the forces and entities it holds responsible for creating and perpetuating existing political, economic, and cultural injustices. Yet unlike many terrorist groups, it has not only gone out of its way to avoid injuring or killing innocent people, but has from the very outset devoted most of its efforts to targeting economic infrastructure. The overall level of violence in Corsica during the past thirty years has been extraordinarily high, especially given the relatively small size of the population and the area it inhabits. Between 1975 and 1999, over 8,000 acts of political violence have taken place on the island. It is therefore not surprising to learn that 63% of the violence that was carried out on all French territory between 1984 and 1999 occurred in Corsica, as opposed to the 5.5% that was attributable to extremist (left- and right-wing) groups, 5% to both the Basques and the Bretons, and a mere 1% to international terrorists. Despite this, and in marked contrast to the 700 deaths attributable to ETA and the over 3,000 attributable to the IRA, the FLNC only seems to have intentionally killed 47 people in the 20-year period between 1975 and 1995 (of whom 18 were rival nationalists, 11 were pro-French anti-nationalists, 11 were Mafiosi, and a mere 7 were policemen); to these totals, a small but unspecified number of inadvertent victims of FLNC bombings must of course be added.[297] The overwhelming majority of FLNC attacks targeted property, buildings, and other material goods rather than the forces of order or individuals, and those attacks were generally very selective. For example, of the 805 such attacks launched between 1976 and 1978 – the first two years of the organization's existence – 166 targeted government property and 643 targeted privately-owned property, and of these latter attacks 129 were launched against tourist enterprises and vacation homes, 100 or so of which were owned by foreigners rather than Corsicans. Overall, the main targets were villas and businesses, especially those linked to the economically vital tourist and agricultural industries.[298]

A few examples of such attacks should suffice to illustrate FLNC targeting of CI. It is perhaps noteworthy that the FLNC carried out 21 separate bombings in towns all across Corsica on May 4, 1976, the night before the official announcement of its formation, since these dramatic and near simultaneous acts seem to have established an operational pattern that was regularly adopted thereafter by the group. For example, on June 18, 1984, the FLNC set off 17 bombs in different regions, targeting banks, tax offices, gas and electricity companies, and real estate offices.[299] On March 21, 1987, the group detonated 41 bombs in northern and southern Corsica on the eve of regional by-elections.[300] More recently, on February 2, 1997 the FLNC – Canal Historique carried out 61 bombings of post offices and tax offices in the north, in part to protest the recent arrest of three of the group's

---

[295] For this pattern of internal factionalization, see *ibid*, pp. 126-7. Compare Rossi and Santoni, *Pour solde de tout compte*, pp. 29-34. They also claim (p. 29) that the group only consisted of a total of about 100 operational members.

[296] Crettiez, *Question corse*, pp. 115, 122, 126, 129. It may also be that the lack of tangible assistance and resources provided by the leadership directorate caused local cells to select easier targets to attack, just as a lack of external funding may have forced them to blackmail or attack economic targets. See *ibid*, pp. 119, 122-123.

[297] For these figures, see *ibid*, pp. 103, 105-08.

[298] *Ibid*, pp. 104, 109-12.

[299] CIP Database #3374.

[300] CIP Database #3590.

leaders.[301] The fact that the organization regularly carried out a series of near simultaneous bombings demonstrates a considerable degree of both operational sophistication and coordination, despite its ostensibly localized, fragmented, and factionalized character.

To sum up, the FLNC's regular targeting of CI has been perfectly *rational* given its ideological opposition to specific French economic policies that have indisputably harmed native Corsicans, *instrumental* insofar as it was designed to achieve tangible and practical objectives by damaging vital industries, *carefully calibrated* in terms of the levels of violence employed, and *highly selective*.[302] Although the group's targets have also often been symbolically representative of various external and internal forces it views as having damaged Corsican interests, there is no doubt that its primary purpose was to *damage materially* those economic industries that had served to perpetuate the second-class status of native Corsicans, above all the tourist industry, agribusiness on the Eastern Plain, and real estate investment in desirable coastal regions by French settlers, vacationers, and other foreigners. In placing such a high priority on attacking these targets, its aim was not only to destroy vital "colonial" components of the island's infrastructure, but also to force resident "speculators" and "exploiters" to leave the island and to warn future would-be investors and purchasers of property that they should look elsewhere if they wished to avoid violent retaliation. These particular objectives grow directly out of the rather unique local conditions existing on Corsica, and, in that sense, the FLNC model may not be entirely applicable elsewhere. On the other hand, the general objectives of the armed nationalist resistance groups in Corsica are not radically different from those of violent nationalist and separatist organizations in places like the Basque Country and German-speaking South Tyrol, in the sense that their primary aims are to preserve their unique culture and establish effective political and economic control over their own homelands.

Chukaku-Ha

Chukaku-ha (Nucleus Faction or Middle Core Faction) is a radical Marxist organization that operates exclusively in Japan. It traces its origins to the Kakukyodo (Revolutionary League of Communists), a group of left-wing extremists that split from the Japanese Communist Party (JCP) in the late 1950s because of the Party's decision to seek socialist revolution through the existing Japanese parliamentary system rather than by means of violence.[303] According to its own literature, Chukaku-ha's "ultimate aim" is to "achieve a communist society through the Anti-Imperialist Anti-Stalinist World Revolution." Towards this end, the group officially supports the "violent overthrow of the imperialist state powers by proletarian armed uprisings."[304] By the mid-1990s, Chukaku-ha, with an estimated 3,500 members, was the largest domestic expressly militant group operating in Japan.[305]

Chukaku-ha has an active political wing, popularly referred to as its "public sector," which is devoted to the development of a viable workers' party alternative to both the Japanese Social Democratic Party and the Japanese Communist Party.[306] The organization also maintains a "hidden sector" – a small, covert military wing of 200-400 members called the Kansai Revolutionary Army or "Revolutionary Force." While it has not engaged in any significant terrorist activity since 1996, this militant core conducted sporadic guerrilla actions from the 1970s to mid-1990s. Its activities were often timed to coincide with overt Chukaku-ha political demonstrations and were primarily aimed at protesting Japan's monarchy system, the American-Japanese security relationship,

---

[301] CIP Database #2581.

[302] Crettiez, *Question corse*, pp. 108-18.

[303] See Peter J. Katzenstein and Yutaka Tsujinaka, *Defending the Japanese State: Structures, Norms and the Political Responses to Terrorism and Violent Social Protest in the 1970s and 1980s*, (Ithaca, NY: Cornell University, 1991), p .26.

[304] Chukaku-ha website, which can be found at: www.zenshin.org/english_home/nc_intro.htm.

[305] U.S. Department of State, *1996 Patterns of Global Terrorism* (Washington, DC: Government Printing Office, 1997), as found at: http://www.state.gov/www/global/terrorism/annual_reports.html.

[306] By the early 1990s, the organization had fielded candidates in numerous local elections and won several dozen seats, including on the Tokyo Metropolitan Assembly.

and other, more specific matters – such as the expansion of Tokyo International Airport at Narita – that were deemed to be particularly important to key constituencies such as students, farmers and union members.

Although Chukaku-ha's attacks have involved a variety of sophisticated tactics and weapons, including automated flame-throwing vehicles, time-delayed bombs, and crude rockets, the majority of its actions have targeted property rather than people. Indeed, the group's attacks on communications, government, and transportation facilities, especially during the late 1970s and mid-1980s, serve as examples of some of the most carefully coordinated and consequential CI-specific terror attacks ever conducted. Of particular note are two attacks made by the group on the government-run Japanese National Railways (JNR) system in 1985 and 1986. Before examining these attacks more closely, it is appropriate to consider Chukaku-ha and its organizational characteristics in greater detail to understand why such targets may have been particularly appealing to it.

As an organization, Chukaku-ha pursues three overarching goals: the successful instigation of a workers' revolution in Japan and, ultimately, the world; the end of the U.S.-Japan security relationship and the American military presence on Japanese soil; and the end of the Japanese monarchy.[307] Ideologically grounded in Trotskyism, the group seeks to engage all levels of society in its efforts and accepts violence as a necessary aspect of social revolution. Indeed, Chukaku-ha does not try to hide the fact that it has, in its own words, "forged illegal underground organizations, revolutionary military forces and armed self-defense."[308] It rationalizes its embrace of violent protest by arguing that the Japanese government and corporations are tools of American imperialism. (The U.S. military presence is deemed to be the most egregious demonstration of the Americans' ongoing occupation of Japan.) Chukaku-ha members argue that such exploitation justifies the employment of any and all measures to end such a corrupt system.[309]

Inasmuch as critical infrastructure facilities such as U.S. bases and Japanese government structures are symbols of Japan's current political system and situation, they may be considered targets for Chukaku-ha. It is important to note, however, that the group does not appear to have targeted such CI facilities because it was ideologically predisposed to attack critical infrastructure specifically. Similarly, Chukaku-ha's attacks on transportation infrastructure, such as the Narita airport and the JNR railway system, were apparently driven principally by the organization's proclaimed ideological commitment to championing and defending workers – in these two specific cases, the farmers displaced by the Narita airport expansion and the train unionists threatened by JNR's privatization. Again, there is no clear evidence to indicate that such targets were chosen specifically because of their nature as key elements of transportation infrastructure.

In terms of its structure, Chukaku-ha is a militant organization with a well-defined internal structure that is uniquely "Japanese" in style. Its internal decision-making processes emphasize the importance of both political consensus and social rank by balancing "work-group autonomy, vertical structures and consensual decision-making, attention to detail, careful planning, and a remarkable ability to learn from mistakes."[310] In the 1990s the organization's membership consisted of approximately 3,500 members, about 500 of whom were "professional" activists who held no steady jobs. When needed, it was estimated that Chukaku-ha had the ability to mobilize about 5,000 people.[311]

After the Japan's Subversive Activity Prevention Law was invoked in 1969 against Chukaku-ha's leader, Nobuyoshi Honda, the organization established its covert revolutionary force to conduct terrorist activities. This smaller group was made up of several hundred members known only to a handful of leaders.

---

[307] Chukaku-ha website.
[308] *Ibid*.
[309] Gerald Utting, "Veteran Saboteurs Lead Japan Rail War," *The Toronto Star*, November 30, 1985.
[310] Katzenstein and Tsujinaka, *Defending the Japanese State*, p.21.
[311] *Ibid*, p. 21.

According to one detailed analysis of the organization, members of Chukaku-ha's "hidden sector" operate in carefully protected cells:

> "These members are mostly the hard-core activists who were involved in the 'Struggles of 1970.' Many of them have a record of arrest or are on the list of those wanted by the police. These military organizations give top priority to the security of their organizations. No lateral relations among their members are established, and vertical relations are also minimal. The entire system cannot be disclosed even if several members are arrested. These organizations adopt thus thorough defensive measures. No member of a cell knows of or recognizes the members of any other cell. Even within the same cell, members use false names with one another to protect their identity."[312]

The members of these cells are noted by police for "keeping complete silence" when they are arrested.[313]

The unique structure of Chukaku-ha's Revolutionary Force and the large size of the entire organization made it particularly well-suited to attack critical infrastructure targets such the JNR railway system. The organization had both the operational security and specialized human resources necessary to conduct sophisticated guerrilla-type attacks. It also had the manpower to attack CI in a large number of locations simultaneously, thereby damaging the targeted infrastructure far more effectively and systemically than would have been possible by means of a single location attack.

Because Chukaku-ha operates exclusively in Japan, its membership consists of a large, active and relatively cohesive group of individuals. The most engaged members tend to be students under the age of 30, though known members have also included public school teachers and local government employees.[314] Many of these members have been arrested for their activities. In the 1980s, during the time of the JNR attacks, numerous Chukaku-ha senior leaders were original members of the organization from the 1960s who considered themselves "professional revolutionaries."[315]While such demographics provide a population of relatively well-educated and committed activists who are both capable and willing to attack CI, there is nothing in the organization's known demographics to suggest a natural group proclivity to attack critical infrastructure over other targets.

According to a variety of estimates, Chukaku-ha is well-financed and has correspondingly significant access to physical, logistical and human resources.[316] The organization demonstrated its financial strength strikingly in 1981, when it built two multi-story headquarters buildings – one in Tokyo and the other in Osaka – at a cost of 500 million yen. At the time of Chukaku-ha's attacks on the JNR railway system in the mid-1980s, the group was believed by police to have a budget of one billion yen per year, which amounted to more than four million dollars at 1985 exchange rates.[317]

---

[312] *Ibid*, p. 28.
[313] Kyodo News Service, "Radical Guerilla Assaults Stop JNR Train Runs," *Japan Economic Newswire*, November 29, 1985.
[314] *Ibid*.
[315] David E. Apter and Nagayo Sawa, *Against the State: Politics and Social Protest in Japan* (Cambridge: Harvard University, 1984), pp. 131-2.
[316] Apter and Sawa note, for example, that Chukaku-ha's financial resources enabled it to maintain a 40-person "solidarity hut" near Narita airport in the mid-1980s, which had expenditures estimated at several million yen per month. Half a million of this sum was used to purchase gasoline for its fleet of twelve cars and twenty motorcycles.
[317] Apter and Sawa, *Against the State*, pp. 131-2.

The group's funding is thought to come primarily from membership dues, the sales of its three newspapers, and fundraising campaigns.[318] Chukaku-ha maintains a group of professional organizers who help rally and mobilize members and collect funds. According to some reports, workers, students and even wealthy supporters from all parts of Japan help fund the group. Membership fees provide a particularly important source of income. According to one report, Chukaku-ha members contribute a significant percentage of their monthly salaries and 100% of their bonuses to the organization. During the 1980s, such financing enabled the group to support some 500 of its members as "full-time" members, allowing them to forgo jobs and instead focus solely on organizational activities.[319]

Chukaku-ha's abundant resources unquestionably facilitated the group's ability to engage in more sophisticated and more numerous attacks, especially in the context of the number of members available to participate in coordinated efforts. It is not clear – or likely – however, that its resources were a key determinant of Chukaku-ha's decision to specifically target critical infrastructure. As the JNR attacks demonstrate, at least some of Chukaku-ha's CI attacks depended on "low-tech" resources that would have been easily accessible to other, less well-financed and well-supplied groups (such as Molotov cocktails and steel pipes).

Although some of the tools used in its JNR attacks were relatively simple, Chukaku-ha is known to possess advanced technical capabilities that enable it to produce a variety of homemade weapons. The organization has also developed its ability to conduct sophisticated operations that involve the use of stolen vehicles, exchanged license plates and registrations, and physical alterations of participants. The group's use of such tools and tactics has been described by some as a form of "high technology guerrilla" terrorism.[320] Especially during the 1980s and early-1990s, these capabilities provided Chukaku-ha with an operational flexibility that allowed the group to increase the number and types of targets it went after, as well as the types of methods it used for conducting attacks.

While Chukaku-ha has demonstrated an impressive ability to innovate, especially in the context of its 1985 JNR attack, it has also tended to gravitate toward particular types of attacks and tactics. For example, the group tried to replicate the 1985 railway attack on several different occasions, each time with less success. Similarly, it conducted repeated attacks on Narita airport that tended to use the same tactics. Chukaku-ha's ability to innovate certainly influenced its target selection of CI, inasmuch as it has helped to expand the pool of "possible targets" and facilitate the group's ability to successfully attack distributed targets such as rail systems. There is little evidence, however, that Chukaku-ha's level of innovation and technical sophistication were significant reasons by themselves for the organization's targeting CI.

It is important to note that the Japanese political left has been highly factionalized since the Japanese Communist Party abandoned its policy of armed struggle in the mid-1950s. In 1957 Kakukyodo – a Trotskyist, anti-imperialist, and anti-Stalinist organization – was established as a militant alternative to the JCP.[321] This group subsequently split into many smaller sects. Chukaku-ha and its main rival, Kakumaru-ha (Revolutionary Marxist Faction), emerged from this splintering in 1963. While Kakumaru-ha tended to avoid open conflict and focused on the development of its organization and its "New Left" ideology, Chukaku-ha emphasized a more openly militant agenda. The assassination of Chukaku-ha's chairman in 1975 by a Kakumaru-ha activist initiated several years of intense violence between the factions, including Chukaku-ha's murder of 43 Kakumaru-ha members.[322]

---

[318] U.S. Department of State, *1996 Patterns of Global Terrorism*.
[319] Katzenstein and Tsujinaka, *Defending the Japanese State*, p. 27; and Apter and Sawa, *Against the State,* pp. 131-2.
[320] Katzenstein and Tsujinaka, *Defending the Japanese State*, p. 26.
[321] The Japanese Red Army (JRA), which sought to overthrow the Japanese government and end the Japanese imperial system, also emerged from the split in the JCP.
[322] Eugene Moosa, "Hundreds of Police Hunt for 300 Rail Saboteurs," AP, November 30, 1985.

Although the level of violence between the groups had subsided significantly by the 1980s, competition for membership and public support between Japanese militant left organizations remained fierce. In the aftermath of the 1985 JNR attack, some Japanese officials conjectured that Chukaku-ha had targeted the railway system to produce a "spectacular" attack that would attract widespread attention and help it gain stature among other Japanese leftist groups.[323]

While there is no definitive proof that Chukaku-ha's decisions to attack CI on various occasions were deliberate efforts to maximize public impact and raise the organization's stature among possible sympathizers, it is impossible to ignore the fact that, due to their systemic nature, many critical infrastructures likely appear to terrorist organizations as particularly desirable targets because of their potential to cause broad public impact if successfully attacked. This was certainly the effect Chukaku-ha's 1985 and 1986 attacks on the JNR rail system had on the Japanese population. After the event, each of these attacks was widely heralded as the most disruptive and damaging attack of its type ever to occur in Japan. Given the highly factionalized nature of the militant Japanese left and the likely outcome of the attack, the associated prestige Chukaku-ha would obtain from conducting the attack may have been an important factor in the group's decision to select the target.

A critical factor affecting Chukaku-ha's target selection was the group's external relations. Chukaku-ha maintains a wide variety of links with other militant leftist organizations, workers' communities of farmers and unionists, and public sympathizers. Since 1968, the organization has been most closely associated with farmers fighting the expropriation of their land for use in the construction and expansion of Tokyo International Airport at Narita. Although the group began attacking the airport even before it opened in 1978, Chukaku-ha's connection with the farmers became particularly well known after it successfully stormed the airport control tower, set it on fire, and attacked police with Molotov cocktails on the airport's opening day.[324] Undoubtedly, the primary motivation behind Chukaku-ha's attacks on Narita airport was the facilities' direct impact on the farmers, and related little if at all to the airport's intrinsic nature as a critical infrastructure.

Chukaku-ha maintains similarly close relations with the 1,100 member Chiba Doro, the Chiba branch of the locomotive union. It regularly cites its close relationship with Chiba Doro as an example of its ability to "revolutionize" workers.[325] The relationship was established in the late-1970s, when Chiba Doro split from the national locomotive union to protest its national organization's support for Narita airport. During the 1980s, when the Japanese government was considering the privatization of the JNR system, early proposals for the railway breakup called for the elimination of as many as 93,000 JNR workers. Chukaku-ha publicly stated that its attacks on the railway system were demonstrations of solidarity designed to call attention to the union workers' efforts to fight the privatization initiative.[326] Again, it would appear that the group's selection of the railway system as a target was done less because of the target's specific nature as CI, and more because of its symbolic importance and specific connection to the constituency Chukaku-ha was championing.[327]

Chukaku-ha's 1985 and 1986 JNR attacks also demonstrated the organization's remarkably sophisticated knowledge of the target. The group clearly understood which specific rail facilities – across a very wide geographical region – needed to be attacked to disrupt the system's service most effectively. As one study noted, "rather than blowing up or tampering with the physical destruction of one rail, the group focused on the critical

---

[323] Cf. *ibid*; and Katzenstein and Tsujinaka, *Defending the Japanese State*, p. 26.
[324] Katzenstein and Tsujinaka, *Defending the Japanese State*, p. 25.
[325] Apter and Sawa, *Against the State*, p. 146.
[326] Masayuki Takagi, Asahi News Service, December 5, 1985.
[327] In "Radical Guerilla Assaults Stop JNR Train Runs," the *Japan Economic Newswire* suggests that a second goal of Chukaku-ha may have been to influence the trial of Hiroko Nagata, leader of the Extreme Leftist United Red Army. Her hearing was delayed because the attacks prevented her defense lawyer from appearing in court.

node (control circuits) and disabled the entire system."[328] Although no definitive link between the attacks and Chiba Doro was ever established, and despite the union's claims that it was not involved with the incidents, it is difficult to believe that Chukaku-ha's knowledge of the CI and its attack plans were not informed to some extent by sympathetic locomotive union members. The technical expertise that such insiders could provide may well have provided Chukaku-ha with both the conceptual idea for the attack as well as the necessary tactical information to implement it. As such, Chukaku-ha's knowledge of its CI target may have been one of the most important factors contributing to the ultimate "success" of its JNR attacks.

A review of the details of these attacks makes the significance of Chukaku-ha's knowledge of the railway system even clearer. The 1985 attack began shortly after 3 a.m. on November 29, when an estimated 200 to 300 Chukaku-ha saboteurs participated in simultaneous raids on more than 30 JNR-related targets in eight prefectures across Western Japan.[329] These coordinated attacks, which were focused in and around Tokyo and Osaka, included the firebombing of signal boxes, the setting of fires with timed incendiary devices at rail installations (including a major downtown Tokyo train station and a transformer substation in Osaka), and the cutting of signal and communication cables.[330] Additionally, several hundred Chukaku-ha members wearing their trademark white helmets, towel masks, and homemade body armor vandalized numerous train stations by attacking the facilities with steel pipes and Molotov cocktails.[331] To prevent the authorities from responding to the attack effectively, the group jammed police and rescue radio frequencies.[332]

The immediate effects of the attacks were dramatic. The damage done to signal boxes and communications cables incapacitated JNR's switching systems, telephone hookups, and computerized booking operations, and forced the rail authority to stop operating its centralized traffic control office.[333] Nearly 3,300 trains on more than twenty lines were disrupted, effectively halting for ten hours JNR's entire network of publicly operated commuter trains.[334] (On an average day, at the time of the attack, the system carried approximately thirteen percent of all travelers in Japan.)[335] Nearly eleven million travelers – ten million in Tokyo and 800,000 in Osaka – were estimated to have been directly affected by the cancelled train service.[336] Many of these regular JNR commuters sought alternate means of travel and thus compounded regional transportation problems by overwhelming the freeways, privately-operated commuter trains, and subways, thereby causing what was widely reported as "mass confusion" and huge jams in these other systems.

While no injuries were directly attributed to this coordinated attack,[337] the sabotage resulted in substantial, measurable damage for JNR and widespread, less-easily calculated costs for the broader community. JNR lost more than six million dollars in ticket sales alone, numerous railway stations were left heavily damaged by the dozens of fires set by vandals, and one Tokyo station was destroyed entirely by a timed incendiary device.[338] Throughout Tokyo and Osaka, hundreds of thousands of businesses and services were forced to close or reduce

---

[328] Matthew J. Littleton, "Information Age Terrorism: Towards Cyberterror," Navel Postgraduate School, Monterey, CA, December 1995, at: http://www.fas.org/irp/threat/cyber/docs/npgs/ch4.htm#b_japan.

[329] See Toshio Kojima, "Terror Group Threatens Hirohito," *The Advertiser*, February 15, 1986; David R. Schweisberg, "Police Investigating Radicals," UPI, November 30, 1985; and Moosa, "Hundreds of Police Hunt for 300 Rail Saboteurs."

[330] Clyde Haberman, "Sabotage Cripples Japan Rail Lines," *New York Times*, November 30, 1985.

[331] Carla Rapoport, "Saboteurs Hit Japan Railways," *Financial Times*, November 30, 1985.

[332] Littleton, "Information Age Terrorism."

[333] Kyodo News Service, "Radical Guerilla Assaults Stop JNR Train Runs," *Japan Economic Newswire*, November 29, 1985.

[334] See Kyodo News Service, "Radical Guerilla Assaults Stop JNR Train Runs;" and Haberman, "Sabotage Cripples Japan Rail Lines."

[335] David Schweisberg, UPI, November 29, 1985.

[336] Schweisberg, "Police Investigating Radicals."

[337] Twelve police officers were hurt while arresting Chukaku-ha members who were vandalizing train stations.

[338] See Moosa, "Hundreds of Police Hunt for 300 Rail Saboteurs;" and Xinhua General Overseas News Service, "Japanese Rail Traffic Disrupted by Sabotage," November 29, 1985.

activities to levels that could be supported by minimal staff. In Tokyo, for example, 420 public and private schools were closed, and even the Stock Exchange operated with only a third of its normal force.[339]

The long-term effects of the attack were less remarkable. Despite the extent of the sabotage, partial train service on all disrupted lines was restored by late afternoon the same day. Nearly 5,000 police were deployed to regional train stations to prevent further violence. Government and JNR officials quickly announced plans for stronger measures to protect the rail network's 12,500 miles of tracks from future attacks, but acknowledged "that it was impossible to guard the entire system."[340] JNR, which at the time was ten billion dollars in debt, noted that burying or securing all of its signal installations would be logistically difficult and prohibitively expensive.

Although police arrested several dozen Chukaku-ha members – including the organization's 32 year-old chairman and 21 year-old deputy chairman – while they were vandalizing railway facilities, the group at first remained officially silent about its role in the attacks. When Chukaku-ha did claim responsibility, it indicated that its acts were intended as a demonstration of solidarity with the Chiba Prefecture Locomotive Union (Chiba Doro), which had launched a 24-hour strike a day earlier to protest the Japanese government's plan to break-up and privatize JNR. Chiba Doro representatives publicly denied all knowledge of the sabotage, but police indicated that the union leadership had been "strongly influenced" by Chukaku-ha and noted that at least two JNR employees had been arrested as participants in the attacks.[341]

Less than a year after the 1985 attack, JNR's commuter rail system was attacked by Chukaku-ha again. On September 24, 1986, the group severed signal and communication cables in twenty-eight locations around Tokyo, in the process affecting fourteen different transit lines. The attacks disrupted train travel in metropolitan Tokyo and stranded more than one million commuters for a brief time. Investigators indicated that the methods used to sabotage the cables were "identical" to those used in the 1985 attack. The attacks occurred the day before the Japanese Diet was scheduled to establish a special committee on the privatization of JNR, and in advance of a meeting of the national locomotive union to decide whether to sign a non-strike accord with JNR management in an effort to ensure greater job security for its members. Besides affecting the outcome of the aforementioned meetings, Japanese authorities suggested that Chakaku-ha's second strike on the railway was designed to more strongly link the issue of JNR privatization with the expansion of Tokyo International Airport at Narita and to increase public political pressure on Prime Minister Yasuhiro Nakasone's government to halt both efforts.[342]

Chukaku-ha's attacks on the JNR railway system are dramatic examples of its larger pattern of attacks on a broad range of CI targets. In the 1980s, for example, Chukaku-ha was associated with more than 250 terrorist incidents. During this period, the group was responsible for 49% of *all* guerrilla attacks and 85% of *all* bombings committed throughout Japan.[343] Although most of these incidents are not captured by the CrITIC Database due to insufficient availability of data, a large number of these attacks were focused on critical infrastructure such as airport facilities, railway stations, military bases and other public buildings.[344]

A systematic review of the key factors influencing Chukaku-ha's attacks on the JNR railway system suggests that the organization selected its CI targets less for their intrinsic nature as elements of critical infrastructure and more for their specific roles as targets symbolically or directly related to issues the group was seeking to champion. Seen in such light, Chukaku-ha's *ideology* and *external relations* were perhaps most directly tied to its

---

[339] Carla Rapoport, "Saboteurs Hit Japan Railways."
[340] Moosa, "Hundreds of Police Hunt for 300 Rail Saboteurs."
[341] Clyde Haberman, "Sabotage Cripples Japan Rail Lines."
[342] Asahi News Service, "Police Blame Leftists for Transit Sabotage," September 24, 1986.
[343] Katzenstein and Tsujinaka, *Defending the Japanese State*, p 25.
[344] *Ibid*, p. 20.

target selection by influencing its operational objective. It is also apparent that the organization's *size*, *structure* and *knowledge of CI* aided it in conducting its attacks successfully. Notably, it is highly unlikely that an organization without some substantial understanding of a railway's operation could have conducted similar attacks with as much ultimate effectiveness, which was probably due to *insider help*. Finally, despite the lack of explicit evidence, it is reasonable to believe that Chukaku-ha found the "spectacular" impact of its first JNR attack valuable in enhancing its status and reputation as an organization, especially within the highly politicized and *factionalized* community of Japanese militant leftist organizations. It is quite probable that a primary motivation for Chukaku-ha's later attempts at attacking railway-related CI was to duplicate its first success.

The Moro Islamic Liberation Front (MILF)

The MILF is currently the largest Muslim separatist group operating in the southern Philippines. It is not a terrorist group per se in the sense that it is a small clandestine organization that relies primarily on terrorist techniques, such as the rival Abu Sayyaf Group (ASG), but rather a relatively large guerrilla movement that employs terrorist tactics along with a wide variety of other methods in order to achieve its political and military objectives. Although the organization is fighting to establish an independent Muslim state, its pronounced Islamist ideology and close links to transnational jihadist networks such as al-Qa`ida and Jemaah Islamiyah place it primarily in the category of a non-state religious group.

Muslim resistance to foreign control in this region dates back nearly 500 years, when Spanish forces first arrived in force in the mid-16th century and thence initiated their long and often violent series of campaigns designed to Christianize and Hispanize the entire Philippine Archipelago. Since that time the Moros (Philippine Muslims) have been stubbornly resisting the imposition of "infidel" control over the southern Philippine islands of Mindanao, Basilan, and Sulu, which a seemingly endless succession of Spanish viceroys, colonial American governors, and independent Filipino (Philippine Christian) leaders have sought to bring about. Nevertheless, Moroland (the predominantly Muslim portions of the southern Philippines) was increasingly brought into the administrative orbit of the Spanish empire, the American colonial administration, and finally the independent, Christian-dominated Philippine government.[345] Not only were the Moros treated as second-class citizens within the new Philippine state, but officials in Manila sponsored policies of internal migration and economic development that quickly led to the demographic displacement of the Muslim majority in large areas of Mindanao, in the process sparking a renewal of Christian-Muslim hostility.[346] It was in this context, whereby Muslims – who now constitute a mere 5% of the population of the Philippines – were squeezed out of several ancestral homelands and marginalized economically, that the modern Muslim secessionist movement arose. The traumatic psychological event that led to its rapid emergence was the "Jabidah Massacre" of March 1968, in

[345] The term "Moro" has long been an appellation for the Islamized groups from the very same Malay racial group as both the Christian majority in the Philippines and the bulk of the inhabitants of nearby Indonesia and Malaysia. Hence the division between Christian "Filipinos" and Muslim "Moros" is neither ethnic nor predominantly social and cultural (in the broadest sense of that term), but rather historical and above all religio-cultural. Indeed, it is important to emphasize that the term "Moro" was originally applied by the Spaniards to Muslim occupants of the Iberian Peninsula, the descendants of a succession of tribal invaders from Islamic North Africa, against whom they had fought a sometimes brutal seven-century struggle for supremacy – the so-called *Reconquista* – culminating in the capture of Granada in 1492. The very same name was then later applied to those recalcitrant Muslims that the Spaniards encountered in the Philippine Archipelago, and it generally retained the same pejorative significance until Philippine Muslim nationalists appropriated it proudly for themselves, in the process transforming it into a positive appellation. For an overview of the history of Islam in the Philippines, see Cesar Adib Majul, *The Contemporary Muslim Movement in the Philippines* (Berkeley: Mizan, 1985), pp. 9-30.

[346] Cf. *ibid*, pp. 30-2; T. J. S. George, *Revolt in Mindanao: The Rise of Islam in Philippine Politics* (Kuala Lumpur: Oxford University, 1980), pp. 107-21; W. K. Che Man, *Muslim Separatism: The Moros of Southern Philippines and the Malays of Southern Thailand* (Singapore: Oxford University, 1990), pp. 24-5. The latter provides evidence (p. 25, chart) that in 1903 Muslims made up 76% of the population of Mindanao, but by 1980 that proportion had been reduced to 23%.

which several Muslim soldiers who had been secretly recruited into a Philippine Army special operations unit were apparently massacred.[347]

By the early 1970s the principal Muslim group promoting armed struggle, secession from the Philippine republic, and independence for Moroland was Nur Misuari's Moro National Liberation Front (MNLF), an essentially nationalist organization with an Islamic coloring which managed to consolidate many previously disparate Moro fighting bands and for years led the resistance movement against the Armed Forces of the Philippines (AFP) and the Christian vigilante squads with whom the military collaborated. Although the MNLF fought the Marcos government to a virtual standstill by the mid-1970s, Misuari's negotiations with government officials concerning a newly-created Muslim autonomous zone in the south precipitated a series of schisms within the organization. One of the breakaway factions, the New MNLF headed by Salamat Hashim, accused Misuari of deviating from "Islamic" objectives and "evolving towards [a] Marxist-Maoist orientation." It was this group that in 1984 renamed itself the MILF.[348] According to Hashim, the reconfiguration of the New MNLF into the MILF was carried out to "underscore Islam as the rallying point of the Bangsamoro struggle." In a letter to the Secretary-General of the Organization of Islamic Conference, he elaborated further on this theme: "All Mujahideen under the Moro Islamic Liberation Front (MILF) adopt Islam as their way of life. Their ultimate objective in their Jihad is to make supreme the WORD of ALLAH and establish Islam in the Bangsamoro homeland."[349] Yet it was not the MILF's declared intention at the outset to rise up against the Philippine government and wage an armed struggle in order to create an independent state, albeit perhaps only for tactical reasons. Instead, its leaders slowly and carefully built up their forces and gradually Islamized the "liberated" areas under their direct control in preparation for the future creation of an Islamic state in Moroland, whose establishment they viewed as a longer term process. Indeed, in an early 1980s MILF programmatic statement describing its four-point policy of Islamization, organizational strengthening, military build-up, and economic self-reliance, the group initially envisioned a three-phase strategy that its leaders expected would last for fifteen years, but this relatively short time frame was subsequently extended until the year 2050.[350]

However that may be, as time wore on the group's underlying ideology became increasingly radical. This may have been due in large part to external influences rather than specific responses to internal developments within the Philippine archipelago. In the early 1980s, even before the formal establishment of the MILF, the New MNLF sent three batches of its carefully-selected field commanders to undergo military training at camps in Afghanistan, of whom at least 360 underwent a year-long course of military instruction and 180 eventually joined the *mujahidin* to fight. Part of their training apparently involved ideological indoctrination as well as hands-on military training, and given their exposure to this transnational jihadist milieu it is likely that many of

---

[347] A good analysis of the "Jabidah Massacre" is provided by Marites Dañguilan Vitug and Glenda M. Gloria, *Under the Crescent Moon: Rebellion in Mindanao* (Quezon City: Ateneo Center for Social Policy and Public Affairs/Institute for Popular Democracy, 2000), pp. 2-23. What mattered most, however, was what the Moros collectively believed had transpired, not what actually happened.

[348] For the circumstances surrounding the MNLF-MILF split, see *ibid*, pp. 121-4; Majul, *Contemporary Muslim Movement in the Philippines*, pp. 86-7; George, *Revolt in Mindanao*, pp. 261-3.

[349] The above two quotes are cited by Thomas M. McKenna, *Muslim Rulers and Rebels: Everyday Politics and Armed Separatism in the Southern Philippines* (Berkeley: University of California, 1998), p. 208, who argues that these had been the goals of Hashim and his cohorts ever since their student days at al-Azhar, even though for a time they had deferred to Misuari concerning MNLF policies. See also Vitug and Gloria, *Under the Crescent Moon*, p. 122. Hence the name change appears not to have reflected a shift in their fundamental goals, but rather their recognition that Misuari had managed to retain firm control over the MNLF even in the face of bitter factional challenges they helped to launch.

[350] Vitug and Gloria, *Under the Crescent Moon*, pp. 124-5. Cf. Salah Jubair, *Bangsamoro: A Nation Under Endless Tyranny* (Kuala Lumpur: IQ Marin, 1999), p. 187. Note that "Salah Jubair" is the pen name of Mohagher Iqbal, the MILF's Vice Chairman for Information.

these individuals returned with far more radical interpretations of Islam than they had when they departed.[351] Moreover, by the mid-1990s key personnel associated with 'Usama bin Ladin's logistical network in the Philippines were collaborating closely with elements of the MILF, and by the end of the decade foreign members of al-Qa`ida were reportedly training fighters in the principal MILF camps.[352] These Islamist radicals from overseas must have affected, whether directly or indirectly, the views of the MILF members and supporters with whom they were interacting. Indeed, more moderate Muslims, including traditional leaders, many younger professionals, "progressives," and the poor, were highly critical of the attempts by MILF leaders and the younger Islamist *`ulama* with which they were allied to impose stricter and more puritanical interpretations of Islam on the Moros residing in their camps and "liberated" zones, as some Philippine Muslims were secularized but most still practiced a syncretistic type of "folk Islam" that incorporated noticeable pagan and Sufi elements.[353]

Even the MILF's organizational structure, which was considered more effective than that of Misuari's looser group, reflected its pronounced Islamic orientation. Like the MNLF the MILF established an executive body known as the Central Committee, but like the earlier Bangsa Moro Liberation Organization (BMLO) it formed both an Islamic judicial organ – in this case one dubbed the Supreme Islamic Revolutionary Tribunal – and a "legislative" Consultative Council (Majlis al-Shura) where policies could be debated and discussed by the organization's leaders. Under the administrative authority of the Central Committee are a Secretariat subdivided into various functional offices and three (later more) vice chairmen, one for Political Affairs, one for Islamic Affairs, and one for Military Affairs. This last official is responsible for overseeing the operations of the group's armed wing, the Bangsamoro Islamic Armed Forces (BIAF). A similar but somewhat less elaborate organizational structure was also set up by the MILF at the provincial level.[354] The BIAF subsequently evolved from a loosely-organized guerrilla force into a 12,000-15,000 strong semi-conventional army consisting of a regular infantry force operating under the direction of MILF Chief of Staff Al-Haj Murad Ibrahim; an elite Internal Security Force (ISF) headed by Abdul Aziz Mimbantas, whose functions include policing MILF areas and ensuring that the *Qur`an* is properly observed; and a Special Operations Group (SOG) headed by Saifullah "Muklis" Yunos and established in 1999, which in spite of the public denials of movement spokesmen is generally considered to be the terrorist section of the MILF.[355]

On the ground, mainly on the island of Mindanao, the MILF operates what Hashim characterized as a "parallel government" in opposition to the "enemy administration" (i.e., the Philippine government bureaucracy) in the areas under its control, an apparatus that revolved around 13 major and 33 lesser camps in the countryside and also functioned inside Moro ghettos in urban areas (such as Campo Muslim in Cotabato City).[356] Some of these

---

[351] For this training of MILF cadres, see Zachary Abuza, *Militant Islam in Southeast Asia: Crucible of Terror* (Boulder: Lynne Rienner, 2003), pp. 90-1.

[352] *Ibid*, pp. 95-99; Rohan Gunaratna, *Inside Al Qaeda: Global Network of Terror* (New York: Berkley, 2002), pp. 243-8.

[353] Several authors have noted that moderate Muslims were often critical, at least privately, of the MILF's restrictive doctrines. Compare Vitug and Gloria, *Under the Crescent Moon*, pp. 128-31; and McKenna, *Muslim Rulers and Rebels*, pp. 213-29. For the "folk Islam" of the Moros, see Peter Gordon Gowing, *Muslim Filipinos – Heritage and Horizon* (Quezon City: New Day, 1973), especially pp. 44-102.

[354] Che Man, *Muslim Separatism*, pp. 194-5 (Appendix 4). The BIAF was originally called the Bangsamoro Mujahideen Army (BMA).

[355] For the MILF's military forces, see Vitug and Gloria, *Under the Crescent Moon*, pp.111-12. For the SOG, see Peter Chalk, "Al-Qaeda and its Links to Terrorist Groups in Asia," in *The New Terrorism: Anatomy, Trends and Counter-Strategies*, ed. by Andrew Tan and Kumar Ramakrishna (Singapore: Eastern Universities Press, 2002), pp. 112-13; and idem, "Militant Islamic Extremism in the Southern Philippines," in Jason F. Isaacson and Colin Rubenstein, eds., *Islam in Asia: Changing Political Realities* (New Brunswick: Transaction, 2002), p. 197.

[356] This "shadow" government was more or less clandestine, depending on the locale. See McKenna, *Muslim Rulers and Rebels*, p. 209, where he also quotes a letter written by Hashim. For the number of MILF camps as of 1998, which apparently shifted over time, see Jubair, *Bangsamoro*, p. 216.

were armed camps that functioned exclusively as military and logistical bases, such as Camp Omar in Maguindanao, but the two largest – Camp Abubakar in North Cotabato and Camp Bushra in Lanao del Sur – were extensive, economically self-sufficient entities that housed entire Muslim communities and were intended to serve as exemplars and living models of the "Islamic state" and Islamized society that the MILF eventually hoped to establish throughout Moroland.[357] For example, prior to its partial July 2000 capture by the AFP, Camp Abubakar had developed into a vast 5,000-10,000 hectare complex that extended for forty miles and included parts of seven villages, and within its confines the MILF had gathered together a self-contained Islamic community with a mosque, a religious school, a prison, a military training academy, an arms factory, a solar power source, sophisticated telecommunications equipment, family housing, markets, a fruit nursery, and agricultural plots.[358] Ironically, some of these amenities were financed with development funds provided by the Philippine government, in part to co-opt the MILF and in part to help the security agencies monitor activities inside the camp itself.

Indeed, the MILF has had a long, complex, and shifting history of interactions with the government. At times the two sides have managed to establish a temporary but unstable truce, but on other occasions very heavy fighting has broken out between them. For example, the MILF was unhappy about the terms of the 1996 peace agreement that the government had brokered with the MNLF – and even more so about its subsequent implementation. As a result, certain elements within the MILF began openly promoting the waging of an armed struggle against the government and the creation of a separate Bangsamoro Islamic state as soon as this was feasible. The relationship between the two parties was further complicated and strained due to the growing impact of radical Islamist doctrines on the MILF's leadership cadre, a process that was only accelerated by growing collaboration with al-Qa`ida and regional Southeast Asian Islamist networks like Jemaah Islamiyah (JI: Islamic Community). Although the AFP has periodically launched several partially successful major offensives against the MILF in recent years, at present an uneasy *modus vivendi* exists between the government of President Gloria Macapagal-Arroyo and the organization's leaders, who have prudently moderated their political demands, curtailed the Special Operations Group's violent actions, and publicly sought to distance themselves from al-Qa`ida and other foreign Islamist terrorist groups in the wake of the September 11, 2001 assaults on the United States. Indeed, as part of her ongoing efforts to reach a negotiated settlement with the MILF, the Philippine head of state has so far successfully lobbied President George W. Bush not to have the MILF added to the U.S. State Department's list of Foreign Terrorist Organizations.[359] During an October 2003 visit to the Philippines, the American president even went so far as to praise the leaders of the MILF for their responsible behavior, in marked contrast to his overtly belligerent and hostile remarks about the ASG.[360]

This was all the more surprising given that earlier that same year there had been a dramatic upsurge of violence by the MILF, including outright terrorist attacks (such as the bloody March 4, 2003 bombing at the Davao airport) and a campaign targeting regional CI, after several years of having conducted mainly low-level operations in the midst of carrying on difficult negotiations with the government. In February 2003, under the pretext that they were going after members of a criminal kidnapping-for-ransom group known as the Pentagon Gang, 5,000 Philippine troops launched the so-called "Pikit Offensive" in North Cotabato in an effort to overrun and destroy the MILF's Camp Buliok, where both these kidnappers and foreign terrorists were said to have taken refuge.[361]

---

[357] Che Man, *Muslim Separatism*, pp. 92-4; Maria A. Ressa, *Seeds of Terror: An Eyewitness Account of Al-Qaeda's Newest Center of Operations in Southeast Asia* (New York: Free Press, 2003), pp. 7-10; Vitug and Gloria, *Under the Crescent Moon*, pp. 113-14 (Abubakar only).

[358] *Ibid*, pp. 106-11.

[359] Abuza, *Militant Islam in Southeast Asia*, p. 99.

[360] "Remarks by the President to the Philippine Congress," full text on White House website, October 18, 2003: www.whitehouse.gov/news/releases/2003/10/print/20031018-12.html.

[361] See, e.g., Zohar Abdoolcarim, "The Philippines'Terrorist Refuge," *Time [Asia]*, February 17, 2003; Anthony Spaeth, "First Bali, now Davao," *Time [Asia]*, March 10, 2003.

In reaction to this major AFP offensive, which killed dozens of rebels and ended up displacing hundreds of thousands of people who lived in the region, the MILF launched military counterstrikes that included several major and minor attacks on the power grid of Mindanao. Typical of such attacks was the February 12, 2003 toppling of two National Power Corporation (Napocor) electrical transmission towers in Pagagawan town, which caused power outages in the entire province of Maguindanao and parts of nearby North Cotabato.[362] Still more serious were the attacks on several electrical facilities in Lanao del Norte on February 26, 2003, which resulted in a complete blackout in most parts of Mindanao for several hours and affected major urban centers such as Davao City, General Santos City, Cagayan de Oro, Cotabato, Butuan, and Malaybalay.[363] Perhaps because several of these attacks adversely affected the very Moro inhabitants of the region whose support the organization sought to rally, MILF spokesmen officially denied any responsibility for carrying out these infrastructural attacks in spite of the evidence indicating that its fighters were directly involved. Hence they offered no public explanation of their reasons for attacking such targets.

However, it is easy to infer that these attacks on CI were simply part and parcel of the extensive array of standard guerrilla tactics that the MILF employed against the Philippine military and security forces. In that sense, the case of the MILF – a large Islamist separatist group that exercises direct administrative control over sizeable territories and enjoys considerable popular support in Moroland – differs considerably from the cases of tiny self-styled political or religious vanguards with little or no popular support that resort primarily to terrorism in the strict sense of that term, i.e., terrorist groups proper. The MILF is instead more akin to broad-based "national liberation" organizations like the former National Liberation Front (NLF) in South Vietnam, the FARC in Colombia, and the Front de Libération Nationale (FLN: National Liberation Front) in Algeria, not (obviously) from an ideological standpoint but rather from the standpoint of its methods and techniques of struggle. MILF attacks on CI appear to conform to the overall logic of waging a multifaceted guerrilla or semi-conventional war within a bounded territory, and in that sense their actions may not represent the reasons why transnational Islamist terrorist networks such as al-Qa`ida might decide to make infrastructural attacks on U.S. soil. Despite this, the MILF's recent wave of CI attacks may well be indicative of a growing Islamist interest in attacking infrastructure.

C. The Record of the Past and Likely Future CI Threats

The case studies above were selected in part because they served to illustrate the broader patterns already identified regarding the types of non-state groups that are most likely to carry out attacks on CI. As noted above, nationalist and separatist groups were responsible for most of the infrastructural attacks in the 1960s, whereas left-wing groups carried out most of the CI attacks in the 1970s and 1980s. In the 1990s, and thus far in the new millennium, religious terrorists have surpassed all other types of groups in carrying out CI attacks.

---

[362] "At least 63 people killed in fighting in Southern Philippines," Deutsche-Presse Agentur, February 12, 2003; "AFP: 70 reported dead, Thousands flee as Philippine Muslim Rebels, Army Clash," World News Connection, February 12, 2003; "Southern Philippine Clash on as Rebels Blast Power Relay Gears," Xinhua General News Service, February 12, 2003; Allen V. Estabillo, "Five Napocor Towers in C. Mindanao Bombed," *Businessworld* (Philippines), February 18, 2003.

[363] Luz Baguioro, "Mindanao Blackout: 18m People on the Island in Southern Philippines are Left in the Dark After Muslim Guerillas Bomb a Power Station," *The Straits Times* (Singapore), February 28, 2003; "MILF Rebels Bomb Power Stattion, Topple Pylons in South Philippines," Channel NewsAsia, February 27, 2003; "Philippine Military Highly Alert on Mindanao Power Stations," Xinhua General News Service, February 27, 2003; "Moslem Rebel Attacks Trigger Blackout in Southern Philippines," Deutsche-Presse Agentur, February 27, 2003; "Philippine Transco Expects to Restore Power in Mindanao by Today/Early Friday," AFX-Asia, February 27, 2003; "Southern Philippines in Brownout Due to Destroyed Power Gears," Xinhua General News Service, February 27, 2003; "Militants Attack Philippines Power Station," Japan Economic Newswire, February 26, 2003; Felipe F. Salvosa et all, "MILF Attack Causes Mindanao Blackout (Napocor Tower Toppled Down," *Businessworld*, February 28, 2003; "MILF Rebels Step Up Attacks, Destroy Power Towers in Philippines," BBC Worldwide Monitoring, February 27, 2003. It is unclear whether this attack was carried out using Improvised Explosive Devices or mortars.

Fortunately, there is little reason to suppose that violence-prone nationalist and orthodox Marxist groups will be inclined to attack American CI in the foreseeable future, especially inside the U.S. itself. Nationalist groups, almost by definition, tend to attack infrastructural targets within their own homelands or within the wider territories – at times including the grounds of foreign embassies – of the governments they believe are unjustly occupying and/or exploiting them, as the cases of the FLNC, LTTE, ETA, and IRA clearly demonstrate. The main exceptions to this general pattern have been factions and offshoots of the PLO, which carried out lethal attacks, seizures of hostages, and hijackings all over the world for over two decades in order to publicize their cause. Old-style Marxist terrorist groups have also typically attacked CI within their own nations, or at most on their own continents, despite their professed internationalist orientation. Here the primary exception was the Japanese Red Army (JRA), which carried out several attacks in the Middle East on behalf of "fraternal" Palestinian organizations. More typical are the European "fighting communist organizations," which almost always attacked CI in their own countries or within the confines of Western Europe, and Marxist groups in the Third World, which have also tended to carry out such attacks in their own or neighboring countries. This has certainly been true of the FARC in Colombia and SL in Peru, and it is likewise true of the Maoist terrorist groups operating in Nepal, the Philippines, and India. Moreover, these types of orthodox left-wing groups are increasingly rare, not to mention unpopular, since the collapse of the communist bloc, the end of the Cold War, and the perhaps fatal discrediting of the entire Marxist revolutionary project. What this summary suggests is that, rather than traditional Marxist revolutionary groups, certain new-style extremist groups that have emerged and grown in importance in recent decades are the most likely to carry out attacks on America's CI.

Such groups fall mainly into three main categories: 1) Islamist terrorist groups with a global rather than a narrowly national or regional agenda; 2) domestic right-wing "militias" whose members bitterly oppose both the "New World Order" and the "Zionist Occupation Government" that has allegedly usurped power in the U.S.; and 3) violent fringes of the radical ecology movement, especially those with an uncompromising anti-technology or neo-Luddite agenda (e.g., philosophical "primitivists" and the most extreme proponents of the mystical, technophobic, and anti-rationalist "deep ecology" current). In addition, certain violence-prone groups that have attached themselves to the worldwide and extraordinarily diverse "anti-globalization" movement, in particular small but violent anarchist and neo-fascist factions, may eventually constitute an infrastructural threat. There are a number of indications that these are the milieus from which the greatest danger stems.

Islamist Groups

There are multiple indicators that violent Islamist organizations are increasingly focusing both their attention and actual attacks on infrastructural targets. This was publicly acknowledged by Algerian terrorist Ahmad Rassam in his July 2, 2001 court testimony after he was arrested in connection with the failed "millennium bombing" plot, whose target appears to have been the control tower at Los Angeles airport:

> "[U.S. Attorney Joseph] Bianco: What did the sabotage part of the training [in one of al-Qa`ida's camps in Afghanistan] consist of?
>
> Ressam [sic]: How to blow up the infrastructure of a country.
>
> Bianco: What types of targets were you trained on?

> Ressam: The enemies' [sic] installations, special installations and military installations, such installations such as electric plants, gas plants, airports, railroads, large corporations, gas, gas installations and military installations also."[364]

Other infrastructural targets were explicitly listed in the al-Qa`ida training manual found by British police in an apartment in Manchester. In the section listing the missions required of al-Qa`ida's Military Organization, the following items were listed, all of which in part concern CI:

> "1. Gathering information about the enemy, the land, *the installations* and the neighbors…
> 7. Blasting and destroying *embassies* and attacking *vital economic centers*.
> 8. Blasting and destroying *bridges* leading into and out of the cities."[365]

Bin Ladin himself has repeatedly urged his followers and other jihadists to attack the U.S. economic infrastructure. For example, in one undated statement, he said:

> "Jihad against America will continue, economically and militarily. By the grace of Allah, America is in retreat and its economy is developing cracks ever-increasingly. But more attacks are required. I advise the youth to find more of their [America's] economic hubs. The enemy can be defeated by attacking its [sic] economic centers."[366]

Perhaps most disturbingly, al-Qa`ida spokesmen and operatives have specifically discussed attacking nuclear plants. As Khalid Shaykh Muhammad put it, nuclear facilities were considered a "key option" for attacks by the group.[367] Needless to say, many other references to the importance of attacking CI can be found in Islamist sources.[368]

Nor has this all been loose talk or bluster. On several occasions Islamist terrorists have either carefully plotted or actually carried out significant attacks against infrastructural targets. Even if one excludes the February 4, 1993 World Trade Center bombing, Ramzi Yusuf's subsequent "Bojinka" plot to blow up several American jetliners in flight on the same day, the 1998 bombings of U.S. embassies in Africa, and the devastating September 11, 2001 attacks on the grounds that al-Qa`ida's operatives had multiple motives for carrying them out, it should never be forgotten that members of a New Jersey-based Islamist cell inspired by Shaykh 'Umar ibn al-Rahman, an erstwhile leader of the two deadliest Egyptian terrorist organizations, were convicted in the mid-1990s of planning to bomb the George Washington bridge and the Holland and Lincoln tunnels, amongst other high profile targets.[369] Had this series of planned near simultaneous attacks been successfully carried out, the results could have been catastrophic. In recent years Islamist terrorists have often specifically targeted CI, and indeed there have been several reports of incidents of this type in just the last few months. For example, in the Spring of 2004, Islamists made two coordinated suicide boat attacks on "energy-related infrastructures" in Saudi Arabia, one at the ADB Lummus Global petroleum facility on May 1 and one at the Arab Petroleum Investments Corporation on May 29. These events, together with a series of Islamist attacks on the housing complexes of Westerners working in the country's oil industry, prompted Saudi officials to reassure foreign energy firms that

---

[364] Cited in Ben Venzke and Aimee Ibrahim, *The al-Qaeda Threat: An Analytical Guide to al-Qaeda's Tactics and Targets* (Alexandria, VA: Tempest, 2003), p. 97.
[365] [al-Qā`ida], *'I'alān al-Jihād 'ala al-Tawāghīt al-Bilād* (no publication information), p. 12 of translated version (emphases ours).
[366] Venzke and Ibrahim, *The al-Qaeda Threat*, p. 118.
[367] *Ibid*, pp. 144-5.
[368] See, e.g., *ibid*, pp. 96-7, 99-103,112-30, 133-5, 146-8, 153-6.
[369] United States District Court, Southern District, *United States of America v. Omar Ahmad Ali Abdel Rahman*. For a short summary, see Simon Reeve, *The New Jackals: Ramzi Yousef, Osama bin Ladin and the Future of Terrorism* (Boston: Northeastern University, 1999), pp. 60-2.

their government would be able to protect them from future al-Qa`ida attacks.[370] Similar attacks have been made, both by Ba`thist hardliners and jihadists, against the Iraqi oil infrastructure, such as the July 1, 2004 maritime attack carried out by three suicide boats on the Khur al-`Amaya oil terminal near Basra.[371] Still more recently, Honduran security officials initially reported that a wanted al-Qa`ida terrorist named Adnan al-Shukrijuma or Ja`afar al-Tayyar had planned to plant explosives in the Panama Canal in order to hamper the flow of ship traffic, an action that, if successfully carried out, could have had very serious consequences. Although these initial media reports were later revised, the Panama Canal Authority nonetheless warned ships to tighten their security against possible terrorist attack or risk being refused passage through the canal.[372] Moreover, on June 21, 2004 members of the Groupe Salafiste pour la Prédication et le Combat (GSPC), an Algerian Islamist terrorist group closely linked to al-Qa`ida, detonated a large car bomb at the main electricity plant in the capital Algiers, killing 11 people and doing considerable damage to the facility. Although the blast was originally portrayed as an accident, this successful attack greatly concerned the Algerian authorities and Western diplomats, since it indicated that the GSPC might also be able to penetrate security at the country's vital oil and gas production installations, upon which its economy heavily depends.[373] In short, all the indications are that Islamist terrorists

---

[370] Elaine Shannon, "Learning from Terror Alerts," *Time*, July 14, 2004; "Saudis move to reassure foreign oil firms," World Tribune, May 31, 2004.

[371] James Glanz, "15 Miles Offshore, Safeguarding Iraq's Oil Lifeline," *New York Times*, July 6, 2004. This same article notes that many attacks have also been made recently on Iraq's oil pipelines, which interim Prime Minister Iyad Alawi estimated has cost the nation $200 million in lost oil revenue. These attacks, however, are part of the repertoire of hit-and-run guerrilla tactics being employed by anti-Coalition insurgent groups, as opposed to examples of Islamist terrorism.

[372] "Panama Canal 'targeted,'" *The Australian*, July 1, 2004; Sherrie Gossett, "Panama Canal target of al-Qaida suspect?," World Net Daily, 30 June 2004; "Panama tells canal ships to tighten security," Reuters, July 7, 2004.

[373] Cf. "Blast hits Algerian power station," CNN, June 21, 2004; "Algeria says June blast was car bomb," Reuters, 6 July 2004; Stephanie Irvine, "Algiers blast was 'car bombing,'" BBC News, July 7, 2004. Apparently, one of the group's motives for perpetrating this attack was to retaliate for the recent killing of GSPC leader Nabil Sahrawi by Algerian security forces. This incident suggests that certain other disastrous explosions at industrial facilities which were initially labeled "accidents" may also have been intentionally caused. One of the most worrisome incidents occurred on September 21, 2001 – ten days after the 11 September attacks in the U.S. – when a massive explosion destroyed much of the huge Azote de France (AZF) chemical plant complex near Toulouse. This AZF plant was the largest manufacturer of phosphate and nitrogen fertilizers in France, and the blast killed 30 people, injured 3000, damaged 10,000 buildings, and resulted in 2.3 billion Euros' worth of damage. See "French factory blast kills 17," CNN, September 21, 2001 (for an initial report); and "Ammonium Nitrate Explosion at AZF Toulouse," Utility Engineering website, April 4, 2003 (for a more comprehensive one): www.saunalahti/fi/ility/AZF.htm. Although the French government officially concluded that the explosion that destroyed the facility was the result of an industrial accident, there are certain suspicious aspects of the case that suggest that Islamist extremists might have been responsible. Hasan Jandubi, a French national born in Tunisia who had been hired to work at the plant five days before the disaster and had, the very day before, yelled at French truck drivers displaying American flags in sympathy with the 9/11 victims, was found dead at the scene dressed in two pairs of trousers and four pairs of underpants, "in the manner of kamikaze fundamentalists." An LCI TV investigation later revealed that Jandubi was a member of a small local cell of al-Takfir wa al-Hijra (Excommunication and Migration), one of the most radical of all Islamist terrorist groups, and that two fellow cell members had previously spent time in Afghanistan. When French police finally went to search Jandubi's apartment, they discovered that it had already been completely cleared out and cleaned. Cf. Daniel Pipes, "Terror and Denial," *New York Post*, July 9, 2002; and "Worst French Industrial 'Accident' Probably Terrorism," *Israel Now*, July 9, 2002. For more on the original Egyptian Takfir wa al-Hijra group, see "Egypt," in Barry Rubin, ed., *Revolutionaries and Reformers: Contemporary Islamist Movements in the Middle East* (Albany, NY: State University of New York, 2003). Curiously, during the Winter of 2004 a mysterious new group calling itself AZF sent a series of blackmail letters to the French government threatening to detonate ten explosive devices that its members claimed to have placed on train tracks if they did not receive a 5 million dollar ransom. One rather sophisticated device was subsequently located by French police along a vital train line, but no ransom was ever paid and in the end no serious damage was done. See "French rail terror threat," AFP, March 3, 2004; "No word from French bomb group," Reuters, March 5, 2004; "Explosive found under French railway after threats from mysterious group," Associated Press, March 24, 2004. According to this last source, the letters were sent to French embassies in Muslim countries throughout the world and explicitly threatened to punish France for banning Islamic headscarves in public schools.

are increasingly focusing their attention on infrastructural targets, both in their own countries and beyond. For this very reason, members of the transnational jihadist networks can be expected to attack U.S. CI at some point in the future.

Domestic American Right-Wing Groups

Members of right-wing American paramilitary organizations also pose a significant potential threat to CI in this country. Such people have already attacked infrastructural targets in the U.S., although in most cases those attacks have hitherto been crude and not particularly destructive. The most significant attack that falls broadly within the infrastructural category was Timothy McVeigh's April 19, 1995 bombing of the Alfred C. Murrah federal building in Oklahoma City, but like the perpetrators of the 9/11 attacks and the December 2001 attack on the Indian Parliament, the disgruntled former soldier had multiple and rather grandiose motives for carrying out this action, the least of which was to temporarily disrupt the functioning of the federal government in one Midwestern city.[374] On several other occasions domestic "militias" have carried out attacks on local offices of the Internal Revenue Service (IRS) or other government agencies, as well as filing a host of spurious "common law" legal suits against officials and repeatedly threatening to harm federal, state, county, and municipal employees so as to prevent them from carrying out certain duties they view as inimical to their interests.

Some individuals affiliated with the American far right and militia milieus have openly discussed targeting infrastructure, both in works of fiction and in manuals designed for internal distribution only. For instance, in the recently-deceased National Alliance leader William L. Pierce's apocalyptic 1978 novel *The Turner Diaries*, groups of racist "patriots" manage to destroy the Washington, DC, headquarters of the Federal Bureau of Investigation (FBI) with an ammonium nitrate truck bomb, make a mortar attack on the Capitol Building during a joint session of Congress, destroy the shipping and industrial capacity of Houston with a series of 14 major bombings, destroy a nuclear plant outside Chicago, knock out water and power utilities in Los Angeles, eradicate the city of Charleston, South Carolina with a nuclear bomb, and destroy the Pentagon with a small airplane loaded with a nuclear device, to name only a few of the most significant infrastructural attacks.[375] This book may have reflected little more than fantastic wishful thinking, but it nonetheless provides a window into the thinking of certain segments of the American far right.

Potentially more worrisome is a 6-page February 1997 document entitled "Intelligence Gathering Guidelines" that was issued by Bill Lacy, the self-described National Commander of Central Intelligence Operations for the American Constitutional Militia Network (ACMN), a diverse coalition of paramilitary organizations from fourteen states. This internal bulletin, which was initially distributed along with copies of the Militia of Montana's (MOM) monthly magazine *Taking Aim*, discusses both "passive" intelligence-gathering methods – such as talking to military and law enforcement personnel, observing troop movements and law enforcement activities, and scrutinizing media reports – and "overt" methods such as the development of "assets" who can provide sensitive information about targeted facilities and organizations. According to the document,

---

[374] For the OKC bombing, see especially United States District Court, District of Colorado, *United States of America v. Timothy James McVeigh and Terry Lynn Nichols*. According to the testimony of his erstwhile friend Michael Fortier, McVeigh's motives for carrying out this attack were to kill as many people as possible, above all those who he believed were directly responsible for precipitating the April 19, 1993 conflagration at the Branch Davidian compound in Waco, and "to cause a general uprising in America," since he felt that such an action might "knock some people off the fence and urge them into taking action against the federal government." Cited by Captain Robert L. Snow, *The Militia Threat: Terrorists Among Us* (New York and London: Plenum Trade, 1999), pp. 97-8.

[375] Andrew Macdonald (pseudonym for Pierce), *The Turner Diaries: A Novel* (Hillsboro, WV: National Vanguard, 1999 [1980]), passim.

> "Your [unit intelligence officer] may ask your assets to seek out certain professionals to befriend, and through this friendship extract critical information. He may ask your assets to do a physical recon of various facilities in order to determine floor plans or security procedures."[376]

The same text also encouraged militia members who worked for gas, electric, telephone, or water services to disclose company security procedures so that they would be in a position to "target key installations for the purposes of harassment, disruption and disabling of enemy field communications, water supplies, fuel supplies and make occupation by these enemy troops more difficult."[377] The specific information sought in these intelligence-gathering efforts was listed in a sheet appended to the aforementioned document and presented in the form of the military-style acronym SALUTE, signifying Size, Activity, Location, Unit, Time, and Equipment. This SALUTE scheme was identical to one also distributed in 1995 by the MOM in connection with its initiation of the Un-American Activities Intelligence Committee, yet another intelligence gathering project that MOM had undertaken jointly with a New Hampshire militia group. It then reappeared again in May 1997, in a similar venture sponsored by the Third Continental Congress.

Another militia document that specifically refers to targeting infrastructure is a 68-page photocopied pamphlet dated June 6, 1994 and entitled *OPLAN American Viper*, which was distributed free throughout the right-wing paramilitary underground during the period prior to the Oklahoma City bombing. Apart from providing an apocalyptic Christian nationalist justification for launching an insurgency against the "hidden socialist infrastructure of the federal government," it contains an annex dealing with tactics that suggests graduating from attacks on "soft targets" such as unguarded rail lines, unguarded telephone and radio communications lines and towers, unguarded water supplies, lightly-guarded supply points and storage areas, and other "targets of opportunity."[378] This treatise was subsequently republished with a cover sometime between 1995 and 1997 as *Militia Operation Plan American Viper* by a Posse Comitatus (Power of the County)-affiliated enterprise in Del City, Oklahoma, allegedly in order to "support and defend the Constitution…from all enemies, both foreign and domestic [and to] inform…God's people and true Americans that love America." These pamphlets clearly demonstrate that various domestic right-wing groups have had an interest in attacking infrastructure.

Moreover, as if to underscore the fact that these publications were not meant solely for "entertainment purposes," two individuals previously associated with the Third Continental Congress were arrested on July 4, 1997, as they prepared to attack Fort Hood during an Independence Day open house being held on the Killeen, Texas military base. At the time of their arrest, the group was found with Kevlar vests, rifles, pistols, 1,600 rounds of ammunition, improvised explosive devices (IEDs), and a manual known as the *Militia Soldiers Operations Handbook*.[379] Indeed, in recent years there have been several abortive plots and a few actual attacks carried out against infrastructural targets from this quarter. For example, on October 9, 1995 an unknown group calling itself the Sons of the Gestapo left notes at the scene excoriating the government and claiming responsibility for the derailment of an Amtrak passenger train near Hyder, Arizona, which killed one person and injured 78 others.[380] On July 1, 1996 several members of an Arizona militia organization called the Viper Team were arrested and convicted on federal conspiracy, weapons, and possession of explosives charges after they were caught conducting surveillance on government offices they were considering targeting, including

---

[376] Cited by Michael Reynolds, "Preparing for War," *SPLC Intelligence Report* 86 (Spring 1997), pp. 8-9. I would like to thank the author of this article, a specialist on the American radical right, for the provision of actual copies and background information about this manual and the other texts discussed below.

[377] *Ibid*.

[378] *Militia Operation Plan American Viper* (Del City, OK: United Sovereigns, no date), Annex 2, pp. 30-1.

[379] "Attack on U.S. bases thwarted," *Dallas Morning News*, April 17, 1997. Five other members of the group were also arrested in three other states for plotting to attack other military installations that they believed were being used to train United Nations troops.

[380] Jim Hill, "Sabotage suspected in 'terrorist' derailment," CNN, October 10, 1995.

those housing the FBI, IRS, Secret Service, Bureau of Alcohol, Tobacco and Firearms (BATF), Immigration and Naturalization Service (INS), National Guard, and Phoenix Police Department.[381] On April 27, 1997 three out of four members of a Ku Klux Klan faction were arrested in a plot to blow up a natural gas refinery outside Fort Worth, Texas, in the process potentially killing hundreds of people, in the hopes of creating a diversion for a planned armored car robbery.[382] On April 18, 1998 three members of the North American Militia of Southwestern Michigan, one of whom was also a member of the Aryan Nations, were arrested and convicted on firearms and other charges after it was discovered that they were planning to bomb federal buildings and an interstate highway interchange as well as destroy aircraft at a National Guard base.[383] Perhaps most interesting of all was the plot hatched by Donald L. Beauregard, head of a militia coalition group known as the Southeastern States Alliance, to destroy energy facilities – possibly including a nuclear power plant – and thereby cause power outages in Florida and Georgia, create general chaos, and precipitate martial law in the hopes that repressive overreactions by the government would catalyze a popular revolt.[384]

There seems to be little doubt, then, that domestic right-wing extremists have displayed an ongoing interest in targeting infrastructure, and there is no reason to suppose that this situation will change in the foreseeable future. Fortunately, most of the plots they have so far hatched have been ham-fisted and ineffective, and their organizational and operational security measures have generally been inadequate to prevent the infiltration of government informants. Even so, and despite the fact that the principal threat to America's CI undoubtedly stems from transnational jihadist networks, Texas City homeland security director Bruce Clawson was right to emphasize that we still have to contend with plenty of "home-grown idiots…who might want to do something [to harm our infrastructure]."[385]

Radical Ecology Groups

Radical ecology groups may similarly emerge as perpetrators that pose a particular threat to critical infrastructures. Many of these groups view the environment as intrinsically just as valuable as human civilization and themselves as avatars defending the natural world against the greedy predations of industry. They see the state and its organs (particularly law enforcement officials) as tools of corporate interests. Radical ecology groups, such as the Earth Liberation Front, have in the past decade also become infused with strands of anarchist, anti-Capitalist and various other social revolutionary ideologies, which has broadened their targets and arguably increased their radicalism. At least up until the present time (although there are signs that these groups may be becoming more violent)[386] these groups have claimed to avoid causing any physical harm to human beings. Consequently, almost all their operations have involved attacks against property and these have on occasion included targets that fall within the rubric of critical infrastructure.

Public awareness of this emerging threat was heightened in the early 1990s. In 1989, five activists were charged with the first "officially designated" act of environmental terrorism in the United States. These individuals – including Earth First! co-founder Dave Foreman – became known as the "Arizona Five" for their efforts to

---

[381] Patricia King, "'Vipers' in the 'Burbs," *Newsweek*, July 15, 1996.

[382] The Southern Poverty Law Center, a group that monitors far right activities in the U.S., lists 30 or so right-wing terrorist plots in chronological order between 1995 and 2001 in "Terror from the Right," *SPLC Intelligence Report* 102 (Summer 2001), including this Klan plot.

[383] *Ibid*.

[384] "Accused Militia Leader indicted on Conspiracy, Terrorist and Firearms Charges," AP, December 8, 1999; "Militia Leader Arrested in Nuclear Plot," ABC Newsline, December 9, 1999; and Larry Dougherty, "Leader of militia will admit role in plot," *St. Petersburg Times*, March 10, 2000.

[385] "Man sought for Photographing Texas Oil Refineries," Reuters, July 19, 2004.

[386] For a full discussion of the threat of radical environmentalism, see Gary Ackerman, "Beyond Arson? A Threat Assessment of the Earth Liberation Front" *Terrorism and Political Violence* 15:4 (Winter 2004).

sabotage power lines associated with nuclear power plants and water projects in the state.[387] Less than a year later, on Earth Day 1990, a group identifying itself as the "Earth Night Action Group" toppled a 100-foot transmission tower and two wooden power poles leading from the Moss Landing power plant outside of Santa Cruz, California.[388] The attack interrupted electricity to nearly 95,000 customers in Santa Cruz for two days and nearly caused the death of an individual suffering from Lou Gehrig's disease after the blackout caused her respirator to fail.[389] A communiqué from the group claimed responsibility for the attack, but authorities failed to identify any suspects in the case.

The escalating rhetoric and scope of action of these groups, together with a continued disavowal of human casualties among many of their activists and their disdain for government institutions, make large-scale attacks against critical infrastructure from this quarter a definite possibility.

D. Tentative Conclusions

The case studies presented in this section highlight a number of clearly identifiable factors that seem to have influenced terrorist motivations to attack critical infrastructure. Although by no means exhaustive or definitive, the insights provided by the analysis of these "real life" situations broadly complement and are consistent with the conclusions derived from the DECIDe Framework outlined in Chapter 5. Several factors, in particular, deserve recognition as having played particularly significant roles in the cases considered here. These include (in alphabetical order): CI Characteristics; External Relations; Factionalization; Historical Events; Ideology; Innovation; Knowledge of CI; Operational Objectives; Organizational Structure; and Security Environment.

CI Characteristics, in particular the symbolic nature and functional importance of such targets, appears to figure prominently in target selection. The attack on the Indian Parliament, in particular, reflects the importance some terrorists place on attacking targets that are meaningful to the broader public.[390] As a widely recognized symbol of India's democracy, the parliament was seen by JEM and LET as an ideal target that the group could attack to show its ability to strike at the heart of the Indian government. The terrorists, however, were more interested in killing a large number of parliamentarians than in actually disrupting the functioning of the Indian government.

In the cases considered here, *Relations with External Actors* clearly play an important role in the process of target selection. The most important external actor, of course, is the target audience whose perceptions and behavior the terrorists hope to influence by carrying out a particular attack. It is also necessary for terrorists to consider the effects of such an attack on their supporters, sympathizers, and proclaimed constituencies. For example, Chukaku-ha's avowed support for Japanese farmers and union members, and the group's decision to champion certain issues relating to these constituencies, probably affected its target selection more significantly than any other single factor. Similarly, the targets selected by the FLNC and MILF generally reflected their supposed commitment to the advancement of the interests of, respectively, indigenous Corsicans and religiously-inclined Moros. Other external actors whose interests must be considered are the rival extremist and terrorist groups which are usually viewed as competitors but with whom a terrorist organization might wish to collaborate, at least temporarily. For example, the joint attack by JEM and LET on the Indian parliament demonstrates how

---

[387] Bron Taylor, "Religion, Violence, and Environmentalism," *Terrorism and Political Violence* 10:4, (Winter 1998), pp. 1-42, as found at: http://www.religionandnature.com/bron/TPV%20article.htm.

[388] Littleton as found at: http://www.fas.org/irp/threat/cyber/docs/npgs/ch4.htm#b_japan.

[389] Brian Anderson, "Earth First case against FBI, police about to begin," Contra Costa Times, April 7, 2002, as found at: http://www.fortwayne.com/mld/fortwayne/3018137.htm; and Bryan Denson and James Long, "Eco-Terrorism Sweeps the American West," *The Oregonian,* September 26, 1999, as found at: http://www.oregonlive.com/special/series/ecocrime.ssf?/special/series/ecocrime_story1.frame.

[390] Although not covered in this section, the September 11 attacks are worth noting as a particularly dramatic example in which terrorists carefully selected CI targets that were both symbolically as well as functionally important.

cooperation between terrorist groups can significantly affect the ability of groups to attack certain targets. JEM had never conducted an attack outside Jammu and Kashmir, and it is likely that LET's logistical division was utilized to help overcome certain operational obstacles that might otherwise have prevented JEM from attacking the parliament building. In this latter case, both groups had to consider how the attack might affect their relations with the Pakistani military and intelligence services from whom they had received covert encouragement and support. However, although external relations can at times directly influence target selection, it is impossible to generalize precisely how such relationships might affect CI targeting without undertaking an in-depth analysis of the specific groups, constituencies, and issues involved in each particular case.

Several of the case studies also suggest that a group's degree of *Factionalization* may exert an impact on target selection. In particular, autonomous, localized cell structures and competitive inter-cell dynamics, such as those characteristic of the FLNC, might induce certain cells to launch attacks that inflict more damage or cause more casualties. Similarly, intense competition between different breakaway groups from the same parent organization, as in the case of Chukaku-ha and its rivals, might encourage them to engage in particularly "spectacular" attacks that they hope will generate higher levels of publicity and prestige. While some CI targets may be particularly well suited to achieve such ends – especially because of their "critical" nature – there is generally a broad array of high profile non-CI targets available that might just as easily be attacked to achieve those same results.

Historical Events, especially tactical precedents, are likely to be key factors in target selection. For example, the MILF tactic of attacking power grids was neither unprecedented nor entirely novel. At least three other insurgent groups which the MILF was either aware of or in contact with – the Moro National Liberation Front (MNLF), the Abu Sayyaf Group (ASG), and the communist New People's Army (NPA) – had also conducted similar attacks. It is very likely that these MILF efforts were in part influenced by such precedents.

Ideology appears to be one of the single most significant factors in influencing a terrorist group's target selection. In the case of the FLNC, for example, the organization's ideology, by identifying the categories of targets that it could and could not legitimately attack, established the parameters within which its *Operational Objectives* were determined. Generally speaking, the FLNC has sought to minimize casualties and focus its efforts primarily on infrastructural targets. As a direct consequence, although it has conducted hundreds of attacks, the group appears to have intentionally killed fewer than 50 people between 1975 and 1995. In a similar fashion, Chukaku-ha's Trotskyist ideology appears to have influenced its target selection by emphasizing violent forms of protest against targets that it viewed as symbolically representative of the capitalist interests which the group opposed, or which were directly related to its purported championing of workers' and farmers' rights. The MILF's ideology, too, generally appears to have generally limited its selection of targets to Christians who were perceived to be harming Muslims, along with its Muslim rivals and less-religious Muslims who overtly opposed its puritanical religious doctrines.

A group's level of *Innovation* appears to be an important factor related to its ability both to attack new and unprecedented types of targets and to plan more effective and novel types of attacks which had a greater likelihood of success. Chukaku-ha's initial attack on the JNR system, for example, was unprecedented in its scope and implementation, which may have been one of the reasons underlying its success. (This may be especially true, considering that the group's successive attacks on the system were less effective because Japanese officials were thereafter better prepared to deal with such contingencies.) Similarly, JEM was the first group to introduce *fidayeen*-style attacks in Jammu and Kashmir. The group had carried out a successful attack against the Kashmir State Assembly in 2001, and it attempted to replicate this same tactic with less effectiveness in the Indian Parliament attack.

In several of the case studies, the group's prior *Knowledge of CI* played a significant role in its target selection and attack modalities. In the case of the JNR attack, it is clear that Chukaku-ha's detailed pre-existing knowledge of the rail system allowed it to inflict maximum damage on its target. Indeed, it can be hypothesized that the group's foreknowledge of the transportation infrastructure, which clearly derived in large part from insiders in the form of unionized JNR employees, may have actually enabled it to conceptualize the attack in the first place.

While the FLNC and MILF attacks on CI were typically much less complex, the two groups' firsthand knowledge of both the environments in which their targets were located and the targets themselves clearly facilitated their ability to carry out those attacks successfully.

A terrorist group's overall *Operational Objectives* also unquestionably play a significant role in its selection of CI targets. The FLNC may provide the clearest example of the way in which operational objectives can exert a direct impact on the selection of infrastructural targets. Since the FLNC's announced objectives were to preserve Corsica's unique culture and make it possible for native Corsicans to establish a greater degree of political and economic control over their homeland, the group focused most of its attacks on symbolic infrastructural targets that it viewed as somehow complicit in the perpetuation of the second-class status of the island's indigenous inhabitants. Chukaku-ha's attacks on JNR facilities were also clearly designed to fulfill its operational objectives of raising the public's awareness of the Japanese government's efforts to privatize the rail system. Indeed, the organization's highly successful 1985 attack adversely and directly impacted approximately eleven million people, thereby making those commuters – and, by extension, the rest of the Japanese public – aware of its political aims.

Organizational Structure appears to affect a terrorist organization's capability to attack various infrastructural targets, but it is unclear whether it actually increases a group's propensity to attack CI. Chukaku-ha's large size and cell-based structure, for example, provided it with the manpower, operational capabilities, and operational security necessary to conduct highly effective guerrilla actions that were especially successful against widely-dispersed CI targets such as the Japanese rail system.

Finally, MILF attacks on the electrical infrastructure in the southern Philippines underscore the fact that changes in the *Security Environment* can serve to motivate terrorist groups to undertake attacks against CI. Those 2003 attacks were in large part intended to be a calculated response to the Philippine Army's damaging "Pikit Offensive." Certain FLNC attacks against CI targets also appear to have been consciously timed to forestall or respond to police crackdowns on the group.

In sum, it should be apparent from both the above case studies and from our preliminary assessments of future threats that a wide range of terrorist groups have attacked CI in the past several decades, and that the interest within certain extremist milieus in carrying out such attacks on U.S. soil seems to be growing. However, since terrorist organizations in every category have attacked infrastructural targets, albeit *typically in response to very specific local or national circumstances*, it remains difficult to generalize about which types of groups will be most likely to do so in the future. That Islamist terrorist groups have displayed an increasing interest in attacking CI may simply be a reflection of the fact that they have also perpetrated an ever-increasing number of terrorist attacks of all types, as opposed to having a perverse obsession with infrastructural targets per se. Moreover, since al-Qa`ida remains interested in carrying out spectacular terrorist attacks in the belly of the "Great Satan" in order to highlight the U.S's vulnerabilities, frighten its "decadent" populace, and kill significant numbers of Americans, it is only natural that its leaders would consider attacking vulnerable CI targets here that would be likely to facilitate their achievement of those objectives. This may be all the more true, given the increasing concerns about such attacks expressed publicly by homeland security officials and the media.

Chapter 4: CRITICAL INFRASTRUCTURE TERRORIST INCIDENT CATALOG*

A. Introduction

While a review of the literature and case studies are critical components in the creation of our analytic framework, an analysis of available statistical data is also essential for a study of this type. Indeed, any serious effort at real world inquiry, especially in the behavioral sciences, is strengthened by a robust data set that is representative of the behavior being studied in order to support hypotheses and validate the findings of the more in-depth empirical study.[391] Thus, in order to develop an accurate analytical framework for terrorist attacks against critical infrastructure, a data set that is representative of these particular types of attacks is required. To meet this need CNS created CrITIC, the Critical Infrastructure Terrorist Incident Catalog. This section explores six aspects of CrITIC: 1) the purpose and need for such a database; 2) the collection process used to create it; 3) the database's structure; 4) the methodology used for inclusion of data within it; 5) future possible development of the database; and 6) initial analysis of the existing CrITIC data set.

B. Purpose

There is an unfortunate absence of terrorism data sets in most academic, scientific, and law enforcement circles.[392] In order to support the analytical framework being developed, a data set that can serve as a representative sample of terrorist attacks against infrastructure over a measurable and comparable period of time was required. Such a data set would then be used to analyze, on various levels, terrorist capability and motivation, such as operational techniques and the desired effects of attack. The required data set also demanded the categorization of relevant information into typologies, such as specific motive, claims of responsibility, perpetrator confirmation, the type of infrastructure attacked, and the effects of attacks. Such detailed, coded information could then generate descriptive statistics from which comprehensive statistical analysis of the attacks against infrastructure could be conducted. Moreover, such a data set could also serve to identify future qualitative case studies that might be needed to support any complete empirical study. In short, an effective data set of terrorist attacks against infrastructure was needed, which would be as qualitatively and quantitatively comprehensive as resources allowed.

Although the analytical framework being developed is meant to be applicable primarily to attacks against U.S. infrastructure, due to the relative lack of such attacks, project researchers needed to create a representative sample from the information available concerning terrorist attacks on infrastructure worldwide. This data set could then be used to provide the broadest[393] possible understanding of terrorist motivations, tactics, and trends in attacking infrastructure. Having identified the need for such a database, the project team next examined extant terrorism databases to see what they offered in response.

---

* This chapter was prepared by Praveen Abhayaratne, Charles Blair, Sundara Vadlamudi, and Sean Lucas.

[391] Colin Robson, *Real World Research: A Resource for Social Scientists and Practitioner-Researchers* (Oxford: Blackwell Publishers, 1993), pp. 3-5.

[392] Raymond A. Zilinskas, "Bioterrorism Threat Assessment and Risk Managements Workshop: Final Report and Commentary," Presented to the U.S. Department of Energy, Monterey Institute of International Studies, June 24th 2003.

[393] As opposed to deepest.

C. Data Collection Process

At the outset, the project team identified an initial list of sources that could be mined for potential data on terrorist attacks against critical infrastructure. Eight relevant sources were identified: 1) the RAND St. Andrews Terrorism Chronology; 2) the RAND-MIPT Terrorism Incident Database; 3) the Center for Defense and International Security Studies (CDISS) Terrorism Database;[394] 4) the terrorism chronologies prepared by Edward F. Mickolus;[395] 5) the International Policy Institute for Counter Terrorism (ICT) Terror Attack Database;[396] 6) the United States Department of State Reports on Patterns of Global Terrorism;[397] 7) the CNS WMD terrorism database; and 8) the CNS Conventional Terrorism Database. Following the identification of these sources, project researchers then carefully examined each source, using a variety of criteria.

First, the comprehensiveness of each source was assessed in relation to reporting acts of terrorism against infrastructure, the time period covered, and the level of detail of the information provided. Second, the project team was mindful that all terrorist operations can involve four broad levels: blueprints and plots; aborted operations; thwarted operations; and successful operations. While ideally data from all four are necessary to attempt to forecast terrorist events, most nongovernmental agencies do not have access to information regarding the first three.[398] In the end, each of the sources was scrutinized in terms of how well it identified the following key target types in its accounts of incidents of terrorism. These were as follows: *airports, banks, chemical plants, communications facilities, dams and waterways, food production / storage facilities, hospitals, military bases and police stations, oil and gas facilities, power plants (electric and nuclear), public service/government offices, roadways, railways, schools, or water treatment facilities.*

It was immediately evident that most sources did not provide the detailed, categorized, or comprehensive information needed for the current study. For example, the RAND St. Andrews Terrorism Chronology and the ICT Terrorism Database did not identify terrorist motivations (i.e., religiously, politically) or the impacts of the attack. Moreover, the latter only covered incidents from 1986 to the present and, while updated on a monthly basis, did not have the requisite incident detail for our purposes. The CDISS Terrorism Database offered only snapshots of terrorist incidents as it was not designed to be comprehensive. Even in-house sources—CNS' WMD Terrorism Research Project Conventional Terrorism Database and its WMD terrorism database—had their limits in terms of infrastructure related attacks.

Not all sources, however, were inadequate. The aforementioned CNS Conventional Database, while chronologically limited (since it covers only 2001 and 2002), was thorough and well categorized. The Monterey WMD Terrorism Database documented information regarding terrorism attacks involving chemical, biological, radiological and nuclear materials from 1900 to the present, from which the project researchers were able to glean relevant information. The Mickolus books also offered data that was comprehensive and historically broad.

---

[394] Located at: http://www.cdiss.org/terror.htm.

[395] The so-called Mickolus chronologies are comprised of four books:
1) Edward F. Mickolus, *Transnational Terrorism: A Chronicle of Events, 1968-1979* (London: Aldwych Press, 1980). (No Edition);
2.) Edward F. Mickolus, Todd Sandler, Jean M. Murdock, *International Terrorism in the 1980's: A Chronology of Events* (Iowa State University Press/Ames, 1989), Vol. 1, 1980-1983. First Edition;
3.) Edward F. Mickolus, Todd Sandler, Jean M. Murdock, *International Terrorism in the 1980's: A Chronology of Events* (Iowa State University Press/Ames, 1989), Vol. 2, 1894 – 1987. First Edition;
4.) Edward F. Mickolus, *Terrorism, 1988 – 1991: A Chronology of Events and a Selectively Annotated Bibliography*, Bibliographies and Indexes in Military Studies, Number 6 (Greenwood Press, 1993).

[396] http://www.ict.org.il/.

[397] http://www.state.gov/s/ct/rls/pgtrpt/.

[398] Joshua Sinai "ICT Conference: Expert on Value, Methods of Forecasting Terrorist Incidents," FBIS Report, Document ID: GMG20031202000085, September 9, 2003.

Yet no *single* source was adequate. Consequently, the decision was taken to build our own database of critical infrastructure attacks – hereafter referred to as CrITIC (the Critical Infrastructure Terrorism Incident Catalog). During its creation, the project team relied most heavily on the Mickolus terrorist chronologies. While these chronicle incidents from 1948-2001 involving violent non-state actors, our second source, the CNS Conventional Terrorism Database, provided detailed incident data for the years 2001 and 2002. However, as is typical of terrorism databases, these data sources used different criteria for the inclusion of incidents and information. Moreover, they were not created specifically with critical infrastructure attacks in mind. Therefore, each incident needed to be evaluated before being entered into CrITIC. When confronted with information deficiencies with respect to particular incidents, project researchers resorted to CNS research and archival resources to conduct further investigation. Unfortunately, for most incidents occurring prior to 1980, there was little further information available in open sources. In these cases, project researchers were as inclusive as possible with available data. The initial population of CrITIC, from preliminary search to final entry, spanned the period from March 9, 2004 to June 15, 2004.

CrITIC is unique in that it brings together critical elements that, when used synergistically, allow for the reliable interpretation of data regarding CI and terrorism. Three fundamental elements of the database should be mentioned. First, CrITIC is populated with a large data set of specific information consistent with the needs of a study addressing the motivational aspects of terrorism. Such an expansive data set allows for the creation of cogent and reliable "large N" studies. Second, CrITIC covers an expansive time-frame—using data from 1933 to 2004. Third and most importantly, CrITIC is populated with incidents that specifically involved CI.

D. Database Methodology

Having obtained the appropriate data, the project team then sought to structure it in an optimally useful fashion. Given the need to allow for quantitative systematic observations of the data, it was necessary to employ the use of a categorization that would allow researchers to generate statistical analyses from the empirical record. In order to do this, coding schemes that contained predetermined categories for recording what was observed had to be created.[399] CNS's experience with designing and populating databases for similar purposes proved advantageous in this regard.[400] Consequently, the project team was able to employ the use of existing coding schemes (e.g. terrorist categories, types of attack, delivery method) used in these databases and effectively develop those needed specifically for the current study. These additional coding schemes or database categories were determined and standardized after careful analysis and discussion by CNS staff to resolve ambiguity as clearly and consistently as possible for the areas of enquiry that the project covered.

As a result of this coding scheme, a typical record in the database has the following eighteen fields of information (See Figure 4.1):

1. **Date of incident:** Exact date of the incident. In the case of ongoing incidents (e.g., hostage situations or kidnappings), the starting date of the event is used.

2. **Location:** City, region or province where the incident occurred.

[399] Robson, *Real World Research,* p. 206.

[400] Both CNS' Conventional Terrorism Database and its WMD Terrorism Database have been specifically designed for the purpose of quantitative analysis of the empirical record.

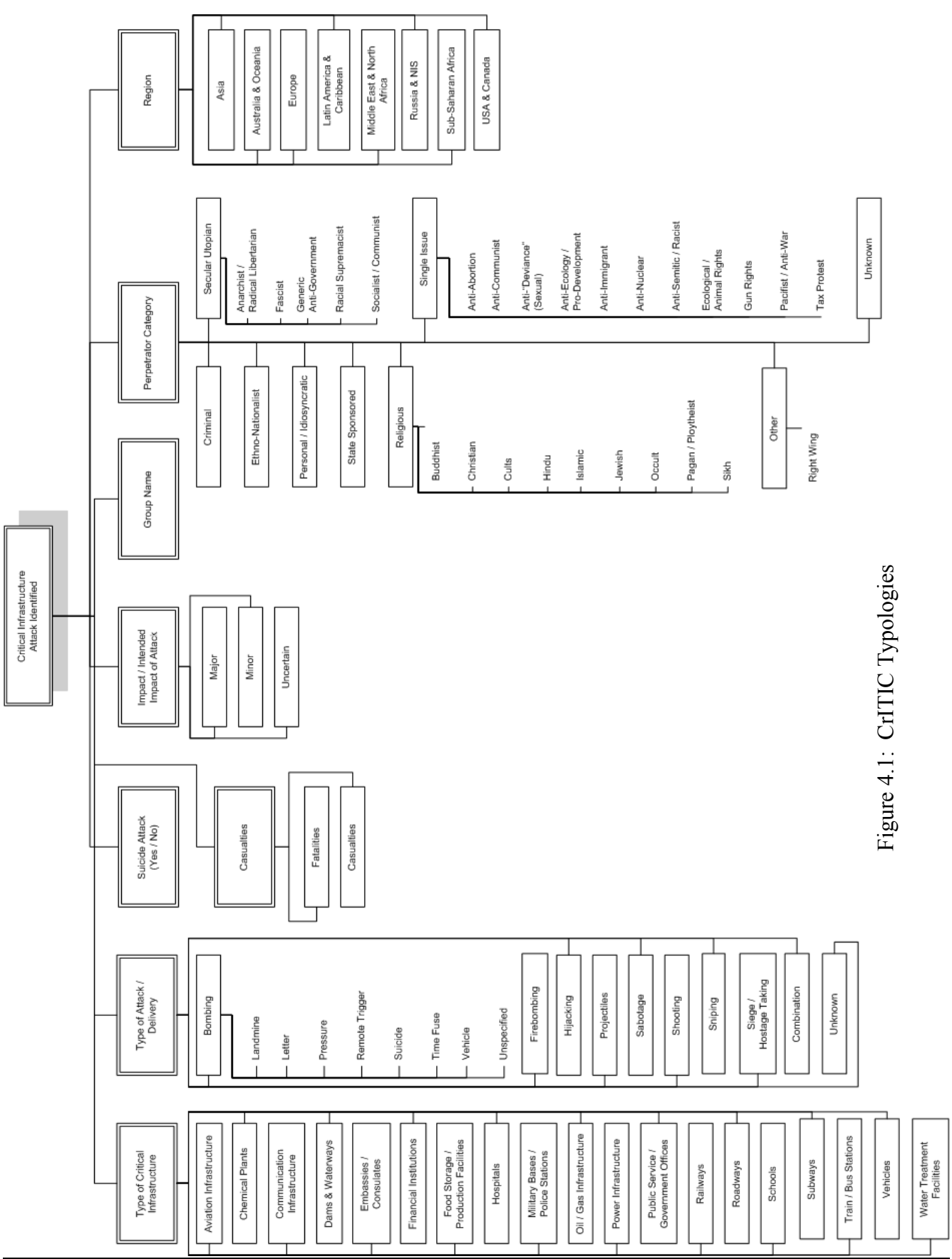


Figure 4.1: CrITIC Typologies

3. **Country:** Country where the incident occurred. This includes only countries recognized by the United Nations. When an incident occurred in international waters or airspace, the country of departure is listed as the country of the incident. In the case of an airplane bombing, the country where the plane crashed is listed as the country of the incident. In cases where hostages were taken, the country where the incident concluded is listed.

4. **Region:** The region of the incident. Regions are divided into the following categories: USA/Canada, Latin America & Caribbean, Asia, Europe, Middle East & North Africa, Sub-Saharan Africa, Russia & the Newly Independent States(NIS), Australia & Oceania.

5. **Target:** Specific infrastructure (target) attacked.

6. **Infrastructure attacked:** Financial institutions, schools, military base and police stations, embassies & consulates, vehicles, public service/government offices, water treatment facilities, dams & waterways, food storage facilities, chemical plants, hospitals, aviation infrastructure, train/bus stations, subways, roadways, railways/roadways/rail lines, communication infrastructure, oil/gas infrastructure, power infrastructure, and other.

7. **Type of attack:** Projectiles (grenades, mortars, missiles); sniping; shooting; sabotage (e.g., arson); hijacking; siege & hostage taking; firebombing (Molotov cocktails, etc.); bombing (landmine, letter, vehicle, timefuse, pressure, remote triggered, suicide, unknown); combination; and unknown.

8. **Fatalities:** Number of confirmed fatalities.

9. **Injuries:** Number of confirmed non-fatal injuries.

10. **Nature of incident:** Domestic or international in nature in relation to the perpetrator. Determination of the nature of a specific incident relates directly to its intended target audience. For example, did the terrorists have a domestic audience in mind, or did they seek to address an international audience.

11. **Perpetrator Group:** Name of group, if known.

12. **Perpetrator Categories:** Ethno-Nationalist(Ethno-Nationalist); Secular Utopian; Religious; Single Issue; State Sponsored; Criminal; Personal/Idiosyncratic; Identifiable but Outside Existing Categories; Unidentifiable.

13. **Perpetrator Sub-categories:** Socialist/Communist; Anarchist/Radical; Libertarian/Anti-Authoritarian; Fascist; Racial Supremacist/ Racial Separatist; Generic (Non-Religious) Anti-Government, etc; Buddhist; Christian; Hindu; Islamic; Jewish; Occult; Pagan/Polytheist; Sikh; Cults; Ecological/Animal Liberation/Primitivist; Anti-Nuclear; Anti-Abortion; Tax Protest; Gun Rights; Anti-Communist; Anti-Immigrant; Anti-Semitic; Anti-Homosexual/Sexual Deviance/Prostitution; Right-Wing; None.

14. **Claim Responsibility** (Checkbox**):** Checked if the perpetrator claimed responsibility for the attack.

15. **Suspected/Unconfirmed** (Checkbox): Checked if a perpetrator is suspected by either external observers or project researchers of carrying out the attack, but there is no evidence to definitively substantiate this.

16. **Summary of Incident:** Concise summary of event, including the date of the incident. The summary also includes information covering the "where, what, why, whom, and how" of the incident. Unusual factors, such as a shift in tactics, the reappearance of an organization, the emergence of a new organization, attack carried out on a historical date, or an escalation of a violent campaign are noted, if available.

17. **Optional Comments:** Supplemental information of importance, such as multiple attacks in the same area or by the same perpetrator.

18. **Infrastructure Impact** (Checkboxes): Major, Minor, Uncertain, N/A.

Coding Scheme

Criteria for Inclusion of Data

CrITIC includes incidents based on the following criteria:

1) The incident had an effect on critical infrastructure (intentionally or inadvertently); or
2) The incident could have had an effect on critical infrastructure (either intentionally or inadvertently) but did not; or
3) The perpetrator(s) intended the incident to have a major impact on critical infrastructure.

Because open sources are unable to provide a representative sample of attacks, cyber infrastructure attacks are not recorded in the database.[401]

Definition of Critical Infrastructure

The following definition of critical infrastructure was used for inclusion of incidents in CrITIC. This definition was developed based on its inclusive nature as compared to other definitions, the use of which would have excluded incidents the project team thought worth recording.

> **Critical infrastructures are those physical systems that a community depends on to maintain its security, governance, public health and safety, economy and public confidence. The constituent parts of such systems will vary according to the community context in which they are viewed.[402]**

Categorization of Infrastructure Attacks

Infrastructure categories were developed by the project team based on the requirements of the study. In certain cases an increased degree of granularity, as compared to existing government infrastructure categories, was deemed necessary in order to better clarify the range of infrastructure targets that have been attacked by terrorists. For example, transportation infrastructure was broken down into multiple categories because the attack methods needed to attack aviation infrastructure, for example, are quite different than those that can be used to attack a train or bus station. In addition, attacks on vehicles were differentiated from attacks on stationary transportation facilities. Similarly, military bases and police stations were combined into a single category, given that the current study is primarily motivational in nature and from a terrorist's perspective both types of installation are likely to be regarded as elements of the security apparatus.

---

[401] In addition, cyberterrorism, which exists largely on the virtual plane, differs in many respects from physical infrastructure attacks. Consequently the same database would have difficulty recording the salient information from both types of attacks. However, where cyber-based attacks had physical effects on a physical infrastructure, the incident was recorded under the category of the physical infrastructure.

[402] See Chapter 1: Defining Critical Infrastructure.

Terrorist Categories with Corresponding Sub-Categories

For the purposes of the database, the following categories were employed for terrorist group types. We believe that the scheme we have employed is considerably more refined than the standard division into nationalist/separatist, left-wing, right-wing, and religious terrorists.[403] Even so, most of the categories we use are clear, if not entirely self-explanatory. The one major exception is that diverse groups that are normally labeled "right-wing" – in the broadest and most casual sense of that term – are here divided among several different categories. For example, neo-fascist and neo-Nazi groups, which incorporate both right- and left-wing ideological components into their worldviews and have an undeniably revolutionary political agenda, are listed under the "Secular Utopian (revolutionary) Groups" category. Domestic US "militia" groups that are essentially secular fall into the "Generic (Non-Religious) Anti-Government" subcategory within this "Secular Utopian Groups" category, whereas those espousing idiosyncratic Christian or pagan Odinist doctrines appear under the "Religious Groups" category. Right-wing groups whose focus is almost exclusively on single issues, such as opposition to abortion, opposition to communism, or opposition to immigrants, fall within the "Single-Issue Group" category. Finally, those that cannot be clearly placed into any of these other categories are placed in the "Right-Wing" subcategory of the "Other" category. For example, members of Latin American "death squads" are not utopian revolutionaries (like fascists), are not usually motivated by religion (like Catholic Traditionalists or Protestant Evangelicals, although they may well be Catholic or Protestant), and are not concerned solely with a single issue (although anti-communism has in the past been one of their principal motivations); thus, there is essentially no other clear category in which to place them. This particular facet of our scheme may seem unduly complicated, but if one genuinely wishes to distinguish between groups with quite distinct worldviews, it is necessary to place them in separate categories. Finally, it should also be kept in mind that many existing terrorist groups (or saboteurs) fall into more than one of these broad categories, which in the real world are by no means entirely discrete. In such cases, the perpetrators' predominant ideological orientation was used for categorization purposes.

The primary categories are as follows:

Ethno-Nationalist groups: This category comprises groups relying heavily on terrorism that seek either to establish an independent state for the ethnic, linguistic, cultural, or national community with which they are affiliated, or (especially if they already have their own independent state) to unite all of the members of their community – including those that live in neighboring countries.

Secular Utopian Groups: This category comprises revolutionary groups with secular ideologies which rely heavily on terrorism, seek to overthrow the existing order, and promote the establishment of a largely impossible-to-create revolutionary new society, either on the international or national level, in which internal strife, injustice, oppression, and domestic or foreign exploitation will be eliminated. This may entail the overthrow of the global capitalist system and either the establishment of a "dictatorship of the proletariat" (Marxist-Leninists) or, much more rarely, a decentralized, non-hierarchical sociopolitical system (anarchists) in which everyone works together for the common good, or it may entail the overthrow of the existing "bourgeois" democratic order, the expulsion of parasitic "anti-national" capitalists, and the creation of an organic national community in which everyone works together for the common good (fascists), the establishment of a mono-ethnic enclave in which all members of that group work together for the common good (racial separatists), or the eradication of the world's "evil" rulers (anti-government radicals).

[403] This decision was largely a result of the fact that one of the senior authors of this report has been studying extremist ideologies for several decades and believes most commonly-used categorizations serve only to obfuscate analysis.

Within this category are the following subcategories:

Socialist/Communist (including Marxist, Marxist-Leninist, Stalinist, Maoist, New Left, etc.)
Anarchist/Radical Libertarian/Anti-Authoritarian
Fascist (including Nazi)
(Non-Religious) Racial Supremacist/Racial Separatist
Generic (Non-Religious) Anti-Government/Anti-"New World Order"/Anti-United Nations/"Anti-Imperialist"/Anti-Capitalist/Anti-Establishment (including militias)

Religious Groups: This category comprises groups that rely heavily on terrorism and seek to smite the purported enemies of God and other evildoers, impose strict religious tenets or laws on society (fundamentalists), forcibly insert religion into the political sphere (i.e., those who seek to "politicize" religion, such as Christian Reconstructionists and Islamists), and/or bring about Armageddon (apocalyptic millenarian cults). This type of terrorism comes in five main varieties: 1) Islamist terrorism; 2) Jewish fundamentalist terrorism, primarily inside Israel; 3) Christian terrorism, which can be further subdivided into fundamentalist terrorism of an Orthodox (mainly in Russia), Catholic, or Protestant stamp (which, in the US, is especially aimed at stopping the provision of abortions) and terrorism inspired by the idiosyncratic Christian Identity doctrine; 4) Hindu fundamentalist/nationalist terrorism; and 5) terrorism carried out by apocalyptic religious cults. Within this category are the following subcategories:

Buddhist (Ultranationalist, Apocalyptic)
Christian (Fundamentalist, Christian Identity, Christian Reconstruction, Catholic Traditionalist, Eastern Orthodox, Protestant Evangelical, Liberation Theology, etc.)
Hindu (Hindu Nationalist, Fundamentalist)
Islamic (Islamist, Fundamentalist)
Jewish (Orthodox, Fundamentalist)
Occult (including Satanist)
Pagan/Polytheist (Odinist, etc.)
Sikh (Fundamentalist)
Cults (all types)

Single-Issue Groups: This category comprises groups that rely heavily on terrorism and are overwhelmingly obsessed with one main issue, such as defending animal rights, ending abortion, or protecting the environment. Although their members often have broader (and often fairly extreme) political views and other matters on their minds, their violence is primarily directed at affecting the one issue upon which they are obsessively focused. Within this category are the following subcategories:

Ecological/Anti-Technology/Primitivist/Animal Liberation
"Pacifist"/Anti-War
Anti-Nuclear
Anti-Abortion
Tax Protest
Gun Rights
Anti-Communist
Anti-Immigrant
Anti-Semitic/Racist
Anti-Homosexual/Anti-Sexual Deviance/Anti-Prostitution
Anti-Ecology/Pro-Development

Criminal Groups: This category comprises groups that rely in part on terrorism, lack discernable political motives, and are principally motivated by criminal goals such as extortion, blackmail, robbery, or perpetrating insurance scams.

Personal/Idiosyncratic Perpetrators: This category comprises individuals (or possibly more than one) who rely in part on terrorism but are motivated by quintessentially personal or idiosyncratic motives that do not conform to standard ideological categories and are usually lost on everyone else. An example might be someone who carried out a violent attack on neighbors because the perpetrator falsely believed that they were somehow conspiring against him or her.

Other Groups: This category comprises anyone else who carries out acts of terrorism but cannot fit into any other category. There is only one subcategory within this category, for the reasons listed above:

Right-Wing

Combined: This category is used when two groups of different types are jointly involved in carrying out a terrorist attack.

State Sponsored: This category is used when a terrorist attack would not have been carried out in lieu of state involvement.

Unknown: This category is used when it is not known who carried out a particular terrorist attack.

Type of Attack/Delivery

Attack types for CrITIC were selected after review of various sources on terrorist weapons and tactics.[404] Only those delivery types that are not self-explanatory have been included in this list.

Hijacking: Hijacking of airplanes, motor vehicles, etc. These may involve hostage taking.

Siege & hostage taking: Attacks conducted for these specific purposes, i.e. to deny entry to an area, and the taking of hostages, not to include hostages taken as a result of hijacking. Thus, in certain incidents, a hijacking was part of the process of taking hostages.

Firebombing (Molotov cocktails, etc.): Crudely improvised firebombs containing highly flammable or explosive materials, such as gasoline, that are easily acquired.

Bombing (landmine): Pressure or timer activated device that is buried in the ground.

Bombing (letter): Letter and parcel bombs delivered to target.

Bombing (vehicle): The use of a vehicle to deliver an explosive device.

Bombing (time fuse): Explosive device placed at the scene of attack that is activated by preset timing device such as a clock.

---

[404] Among other sources the list of Conventional Terrorist Weapons from the United Nations Office of Drugs and Crime. Located at http://undoc.org/unodc/terrorism_weapons_conventional and Christopher Dobson and Ronal Payne, *The Weapons of Terror* (London: McMillan, 1979).

Bombing (pressure): Physical, water, or atmospherically activated explosive devices placed at the scene of attack. Not to include pressure activated landmines.

Bombing (remote triggered): Device placed at the scene of attack that is activated remotely using electronic pulse or signal such as radio, cellular phone, or remote control.

Bombing (suicide): Device delivered by a human that intentionally blows him/herself up in the process.

Bombing (unknown): Unidentified delivery method used for explosive device.

Combination: Attack using a combination of the methods listed in this category.

Unknown: Unidentified delivery method.

Other: Identified but uncategorized delivery method.

Major and Minor Impact

While information regarding major infrastructure attacks is most pertinent, there is also considerable value in tabulating and assessing minor infrastructure attacks, since this can help discern terrorist motivations for attacking infrastructure. Consequently, infrastructure attacks needed to be divided into "major" and "minor." Therefore, in the context of categorizing the attacks in CrITIC, the existing entries have been divided into four separate categories: 1) major infrastructure attacks; 2) minor infrastructure attacks; 3) uncertain cases; and 4) non-infrastructure attacks (N/A).

Only those incidents that a) did have, b) could have had, or c) were intended to have a large-scale (i.e., regional or national, not local) social, political, and/or economic impact were considered "major." The rest, by default, fell into the "minor" category.

Incidents involving critical infrastructure entailing purely economic or psychological effects were included, but only if these affected the functioning of the critical infrastructure itself. That is, even if an attack had a widespread psychological impact, if this impact did not affect the critical infrastructure it would not be included. In some cases the impact of an attack may be unknown because of a lack of evidence in the source documents. In such cases the project researchers processed information according to the following criteria:

a) if investigators were reasonably certain that the incident caused no major impact, and there was no evidence to the contrary, the incident was not labeled a major incident;
b) if (based on general investigator knowledge or the scale/nature of the incident) there was reasonable certainty that there was a major impact, the incident was included as a major incident;
c) if there was uncertainty of the magnitude of the impact, the case was researched further;
d) if there was still insufficient information after research to make a determination, and (b) above did not apply, then the incident was regarded as not having had a major impact.

The entire data set and categorizations were reviewed and corrected (where needed) by two senior researchers at the culmination of the data entry process before any statistical analysis was conducted.

E. Preliminary Data

The database records 1,874 incidents from November 1933 to March 2004. Of these, 188 incidents represented major attacks on critical infrastructure, while only 168 of this subset were confirmed as having been perpetrated by the group(s)/individual involved. There were 895 minor attacks against infrastructure, of which only 765 were confirmed attacks.

F. Further CrITIC Development

Owing to limited available open-source information on certain incidents and finite resources, the project team realizes that for certain incidents the details contained therein may be uncorroborated or lack the requisite detail for proper analysis. For instance, the difficulty in determining the exact impact of an attack resulted in a number of cases being categorized in the "uncertain" category of impact type. The difficulty often lies in determining the nature of the attack, and whether the attacks were perpetrated to make a symbolic statement, to destroy property, or to kill large numbers of people. Therefore, we regard CrITIC as a work in progress, a necessary foundation upon which further development can occur. To achieve this, further in-depth research on select incidents will be required. While preparing case studies for this deliverable, project researchers did conduct further research on selected incidents and were able to supplement the original data. However, this also proved to be a time intensive process, which must be taken into account in making further improvements to the database.

Database Statistical Analysis

Introduction

This section offers a broad overview of the preliminary CrITIC findings, examining five areas at the nexus between terrorism and CI. First, is an investigation of the general number of attacks, specifically, an overview of the total number of attacks recorded in the database in relation to the various categories. The second subsection is a discussion of the different kinds of infrastructure attacked. Identified are the kinds of CI most frequently targeted and how this has changed over time. Third, is an exploration of who the attackers of CI have been. Detailed descriptions are given of the different Perpetrator categories, how incidents involving these groups have changed over time, and which targets they have chosen to attack. The fourth subsection is an analysis of the different methods of attack: with which weapons and delivery systems has CI been attacked? The fifth subsection examines casualties in relation to CI attacks. Attention here is given to the overall numbers and how these have changed over time, which attack methods have resulted in the highest casualties, which groups have engaged in attacks that statistically resulted in the highest number of casualties, and the role played by the type of infrastructure attacked in casualty rates. Finally, the chapter concludes with a summary of general implications concerning motivations for attacking CI.

Prior to exploring this section, the reader should keep several points in mind. 1) It should be noted that, unless otherwise specified, only major and minor attacks will be discussed. 2) In order to avoid introducing researcher bias into the data, only confirmed perpetrators have been discussed when analyzing Perpetrator Category and Group Name categories. 3) The chemical incident in Bhopal and the September 11 attacks in the United States have been excluded from casualty counts given the ambiguity in categorizing these incidents and the exceptionally large number of casualties.[405] 4) Because these statistics were drawn from *international* incidents of

[405] It is still contested whether the incident in Bhopal was due to insider sabotage or an accident resulting from negligence. If the latter were the case, the incident would not be included in the database. Additionally, the extent to which al-Qa`ida's

terrorist attacks on CI, the extent to which they reflect U.S. domestic trends is debatable. 5) For the reasons mentioned earlier, it is beyond the scope of this study to compare trends in terrorism in general with specific attacks on CI. Lacking this contrast, there is the danger that the conclusions drawn below could be misinterpreted. For example, the lethality of CI attacks grew dramatically in the 1990s, yet so did terrorist attacks in general. In short, striking trends in attacks on CI might not appear so dramatic if one is mindful of terrorist attack trends in general.

A series of figures are referenced throughout this section. They provide a visual snap-shot of sometimes recondite trends. *The figures are located in Appendix I (AI).*

General Attack Figures

Total Number

CrITIC contains a total of 1,084 incidents categorized as either major or minor attacks. These incidents account for 58% of all the incidents captured in CrITIC.[406] Of this total, the number of attacks on infrastructure that had a "major" impact was 188 (or 17% of those incidents that were identified as having major or minor impact). Of these, only 168 attacks could be attributed to specific perpetrators.[407] There were 896 attacks that had a minor impact on infrastructure, of which 766 could be attributed to specific perpetrators. Out of the 1,083 incident that had some significant impact on CI, 934 involved attacks that could be attributed to specific terrorist groups.

Frequency of Attacks

CrITIC covered attacks against infrastructure from November 1933 to March 2004. The paltry number of attacks between 1933 and 1970 do not reveal any significant trends. This can be attributed partly to the relative absence of open source reporting as compared with the post-1970s period. It was not until the late 1960s and 1970s that the media began focusing on incidents of terrorism. It is notable, however, that the number of terrorist attacks against infrastructure increased significantly in the years after 1980. The 1980s alone accounted for 471 incidents, or 43% of all major and minor attacks against infrastructure, and 25% of all recorded incidents. The 1990s accounted for 308 incidents or 28% of all major and minor incidents, and 16% of all incidents. Although incidents for only 3.3 years of the 2000 decade are in the CrITIC, the 132 recorded incidents represent 12% of all major and minor attacks. (See Figure AI-1.)

Region

The largest percentage of attacks against infrastructure, 29%, has been carried out in Europe. The next largest percentage of attacks has occurred in the Latin America and Caribbean region, accounting for 26% of all attacks. Almost all of the incidents in both regions are attributable to nationalist or secular utopian (especially extreme left) terrorist groups. (See Figure AI-2.)

---

targets in the September 11th attacks were designed to specifically attack infrastructure and the extent to which they were intended to kill a large number of people is not certain. The large casualty numbers for these problematic cases would in any event skew statistical analysis.

[406] Most of the remaining incidents were classified as "Uncertain" and require further investigation before they can be included in statistical analysis.

[407] Unconfirmed attacks are those in which the perpetrator is suspected of carrying out the attack, but there is no corroborating evidence.

Type of Infrastructure Attacked

Analysis of the type of infrastructure targeted (while controlling for various other parameters like the region of attack, the number of casualties, the type of attack, and the category of the terrorist group that perpetrated the attack) reveals several salient points. Generally speaking, with regards to major *and* minor attacks, the data reveals that attacks against Embassies/ Consulates constituted the bulk of attacks, with 45% of the total number. The attacks against Public Service/ Government Offices represented 14%, with attacks against Financial Institutions constituting 11%. Additionally, Oil/Gas Infrastructure for 9% of the attacks.

Restricting the categorization to include only major CI attacks perpetrated between 1933 and 2004, 50% were against Oil/Gas Infrastructure. With regards to other infrastructures suffering major attacks, Power Infrastructure targets comprised 15%, followed by Public Service/Government Offices, Railways, and Dams and Waterways at 8%, 5.3%, and 3.7% respectively.

Perpetrator Categories and Type of Infrastructure Attacked

Among the terrorist categories where members perpetrated the largest number of the attributable major attacks against CI, Secular Utopian groups come to the fore with 47 attacks. This category is closely followed by Ethno-Nationalist and Religious groups with 43 and 19 attacks respectively. These top two group types – Secular Utopian and Ethno-Nationalist– have displayed a propensity to attack Oil & Gas infrastructure facilities, comprising more than 50% of these groups' total number of major attacks on CI. In contrast, Religious groups have evenly distributed their major attacks over various types of infrastructure.

When the data analyzed included both major *and* minor attacks, Secular Utopian perpetrators again lead the way with 227 attacks. Similarly, Ethnic/Nationalist/ Separatist/Irredentist groups follow with 142 attacks, and Religious groups again come in third with 64 attacks. The largest portion of the major and minor attacks by these three top categories was against Embassies/Consulates. Secular Utopian groups conducted 37% of their attacks against Embassies/Consulates and Ethno-Nationalist groups and Religious groups conducted 29% and 39% of their attacks against Embassies/Consulates respectively. Clearly, these numbers indicate consistency between targeting and the anti-Western and anti-colonial bent of ideologies in these top categories. The Secular Utopian groups conducted 16.7%, 16.3%, and 10.6% of their attacks against Public Service/ Government Offices, Financial Institutions, and Oil/Gas Infrastructure respectively. The Ethno-Nationalist groups conducted 18.3%, 16.9%, and 10.6% of their attacks against Oil/Gas Infrastructure, Public Service/ Government Offices, and Railways/Railroads/Rail lines respectively. Religious groups conducted 15.6%, 6.3%, and 4.7% of their attacks against Public Service/ Government Offices, Financial Institutions, and Power Infrastructure respectively. The variance in these percentages shows that Public Service/ Government Offices were a preferred target between all three categories but no significant preference of infrastructure target selection within groups can be identified.

Regions and Type of Infrastructure Attacked

Attacks on Oil/Gas Infrastructure contributed to more than 50% of the attacks in Europe and Latin America/Caribbean. Significantly, in the Middle East/North Africa region, the attacks on Oil/Gas Infrastructure accounted for 85% of the attacks on CI. The high percentage of attacks on CI in this region could be partly attributed to the vast number of oil and gas infrastructure targets in the region, and the vulnerability of those targets vis-à-vis other CI. In contrast, in Asia the attacks on Oil/Gas Infrastructure constituted approximately 30% of the major attacks on CI.

Time Period and Type of Infrastructure Attacked

The data for major attacks on CI indicate that terrorists have targeted Oil/Gas Infrastructure consistently since 1960. For every decade since 1960, the number of attacks on Oil/Gas Infrastructure has been higher than the number of attacks on other types of CI. As previously noted, a large percentage of the attacks against Embassies/Consulates were categorized as minor attacks and appear as the most frequently attacked CI in general (45%) when including both major and minor incidents. Moreover, the number of attacks against Embassies/Consulates peaked in the 1980s, accounting for 50% of attacks.

Type of Infrastructure Attacked and Casualties

Major attacks on CI produced a total of 1,814 deaths. The number of fatalities caused by attacks on Oil & Gas Infrastructure constituted 36% of this total, while attacks on Public Service/Government Offices represent 25%. Major attacks on Military Bases and Police Stations represent 12%, while Embassies/Consulates accounted for 10% of the total number of fatalities. The set here did not include the Bhopal gas tragedy and the September 11 attacks.

The total number of fatalities caused by both major *and* minor attacks with a confirmed perpetrator on CI was 2,446. The attacks in the Oil/Gas infrastructure category and the Public Service/Government Office infrastructure category led with 26% and 24% of the total number of fatalities respectively. The number of deaths resulting from attacks on Embassies/Consulates, and Public Service/Government Office each contributed about 10% of the total number of fatalities. Military Bases and Police Stations accounted for 11%.

Similarly, out of the 14,099 casualties (a figure that includes non-lethal injuries) produced by major terrorist attacks on CI, the attacks on Embassies/Consulates and Public Service/Government Office each produced 31% and 25% of the total number respectively. Upon considering the data for both major *and* minor attacks on CI, the attacks on Embassies/Consulates and Public Service/Government Office produced 26% and 25% respectively of the 18,066 casualties that resulted from these attacks.

Preliminary statistical analysis of the major and minor cases in CrITIC indicates that the number of casualties varies according to the type of the targeted infrastructure. However, the variation of fatalities, injuries, and casualties between different types of infrastructure was not significant when the data for the Bhopal gas tragedy and the terrorist attacks on September 11, 2004 were excluded from the analysis.[408]

Perpetrator Categories

The total number of major attacks "attributable" to specific groups was 168. Secular Utopian groups carried out 27% of these attacks followed by Ethno-Nationalist groups that carried out 26% of these attacks. Among other identifiable group categories, Religious groups were responsible for 11% of the attacks. (See Figure AI-3.)

The data for attributable major and minor attacks reveals that out of the total number of 933 incidents, Secular Utopian groups remain the most active with 24% of the attacks. Ethno-Nationalist groups follow, responsible for 15% of attacks. (See Figure AI-4.)

---

[408] A one-way ANOVA test was conducted between the types of infrastructure attacked and the mean number of fatalities, injuries and total casualties. See Figure 5 in Appendix III (The SPSS output indicates the test results after excluding the cases of the Bhopal chemical incident and the 9/11 terrorist attacks)

Frequency of Attacks over Time and Perpetrator Categories

Of major attacks by Ethno-Nationalist groups, incidents follow neither a steadily increasing nor a decreasing pattern. The attacks are also not concentrated within any particular time period. Similarly, attacks conducted by Secular Utopian groups are distributed evenly, although an increase in the number of attacks is evident between 1983 and 1987. The distribution of attacks by Religious groups does not follow a steadily increasing or decreasing pattern until the late 1990's when this category becomes responsible for an increasing number of incidents. (See Figure AI-5.)

The distribution of major *and* minor attacks conducted by Ethno-Nationalist groups does not follow any clear trend; however, a perceptible increase in the number of attacks carried out by these groups between 1980 and 1987 is evident. (See Figure AI-6.) The attacks carried out by Religious groups similarly do not follow any steady pattern and the data indicates an apparently randomly varying distribution of attacks. The distribution of attacks by Secular Utopian groups shows an increase in the number of attacks between 1980 and 1988, after which a decreasing pattern of attacks is observed. Recently, however, that the number of attacks by Secular Utopian groups showed an increase in 2002.

Preliminary statistical analysis of data for all the cases in CrITIC reveals that the difference in the mean number of attacks over decades by different types of terrorist groups is statistically significant.[409]

Region Where Attack Occurred and Perpetrator Categories

The distribution of attributable major attacks by Perpetrator category over various world regions reveals several interesting details. In Asia, there were a total of 27 incidents. Attacks by Religious and Secular Utopian groups led the way, constituting 29% and 26% of all attacks respectively, while attacks by Ethno-Nationalist groups accounted for 18.5% of attacks. In contrast, of the 36 attacks in Europe, the vast majority, 47%, were conducted by Ethno-Nationalist groups. Secular Utopian groups conducted 19% of the attacks. Compare this to the Latin America/Caribbean region, where Secular Utopian groups conducted 81% of attacks. In the Middle East/North Africa, there were a total of 25 major incidents. The Ethno-Nationalist groups conducted 32% of the attacks and Religious groups were responsible for 12% of the attacks. In Sub-Saharan Africa, Ethno-Nationalist groups conducted 57% of the 21 major attacks in the region and Religious groups conducted 9.5% of the attacks. Finally, in the United States and Canada, there were a total of 19 major attacks. Interestingly, Religious groups conducted 26% of the attacks (a figure equaled only by the Religious group attacks in Asia). Secular Utopian groups conducted 5% of the attacks. Significantly, individuals in the Personal/Idiosyncratic category were responsible for 31.5% of the attacks against CI in the United States. This figure is far higher than any other region. (See Figure AI-7)

When we consider both major *and* minor confirmed perpetrator incidents, the picture is largely similar. In Asia, we find total attacks numbering 114. Secular Utopian groups conducted 26% of attacks and Religious groups carried out 16% of attacks. Ethno-Nationalist groups accounted for 11% of the attacks. In Europe, Ethno-Nationalist groups accounted for 31% of the 278 major and minor attacks against CI.

[409] A two-way Analysis of Variance (ANOVA) test was conducted to examine the distribution of attacks by various groups over several decades. See Figure 1 in Appendix III.

Secular Utopian groups carried out 24% of the attacks and Religious groups conducted only 2% of the attacks. The relative scarcity of attacks by Religious groups in Europe presumably reflects the fact that historically the region has not been home to many groups whose primary orientation was religious. In the Latin America/Caribbean region, out of 235 incidents, Secular Utopian groups carried out 49% and 42.5% of attacks fell in the Unknown category. Religious and Ethno-Nationalist groups accounted for only 0.42% and 0.85% of the total number of attacks respectively. However, in the Middle East/North Africa region, Religious groups rebounded, accounting for 19% of the 155 major and minor attacks. Ethno-Nationalist groups and the Secular Utopian groups conducted about 10% and about 5% of the total number of attacks respectively. In Sub-Saharan Africa, Ethno-Nationalist groups and Religious groups account for 41% and 4% respectively of the 49 major and minor incidents. In the United States/Canada region, there were 77 major and minor incidents. Ethno-Nationalist groups carried out about 8% of the attacks and Religious groups conducted 10% of the attacks. As was the case when examining major only attacks by groups and individuals with Personal/Idiosyncratic motivations, major and minor attacks were higher in this region than anywhere else globally, accounting for 13% of the total number of attacks. The majority of attacks were perpetrated by unidentifiable perpetrators. (See Figure AI-8.)

A statistical model was created to determine whether a relationship exists between the terrorist categories and the day of attack, the month of attack, and the geographical region of attack. The statistical model utilized the data for all the cases present in CrITIC and concluded only that a correlation exists between the type of terrorist group and the region of the terrorist incident.[410]

Attack Method and Perpetrator Categories

All the different categories of terrorist groups utilized various types of bombing to carry out the vast majority of major attacks against CI. (See Figure AI-9.) The data for both major *and* minor attacks reveals similarly that all groups use various types of bombing to carry out most attacks against CI. The Ethno-Nationalist groups used bombing to conduct 68% of their attacks and used Projectiles and Sabotage to carry out 9% and 5% of the total number of attacks respectively. Religious groups have used bombings to carry out about 58% of their attacks, with Projectiles accounting for 14%. Secular Utopian groups have carried out 59% of their attacks utilizing bombings. Like other groups, they have also relied on Projectiles and Sabotage, which constitute 11% and 5% of their attacks respectively. (See Figure AI-10.)

Perpetrator Category/Sub-Category and Casualties

For major attacks with a confirmed perpetrator, attacks by Religious groups have accounted for 73% of all casualties. Ethno-Nationalist and Secular Utopian groups have accounted for 16% and 11% respectively of the total number of casualties (fatalities and injuries). For attributable major *and* minor attacks, Religious groups have accounted for 67% of all casualties, the vast majority appearing under the Islamic sub-category. Secular Utopian and Ethno-Nationalist groups have accounted for 11% and about 17% of all casualties respectively. (See Figure AI-11 & Figure AI-12.)

Preliminary statistical testing of all major and minor terrorist attacks reveals that different types of terrorist groups do not produce the same number of casualties and that the Religious groups have shown themselves to be the most lethal, though not responsible for the largest total number of fatalities. The number of casualties varies significantly across different types of terrorist groups.[411]

---

[410] Multiple Discriminant Analysis was used to evaluate the relationship between the terrorist group types and the month and region of attack.

[411] A one-way ANOVA test was used to study the variation of casualty levels across different types of terrorist groups. See Figure 4 in Appendix III.

For all confirmed perpetrator major attacks, Religious groups have accounted for 80% of all injuries and Ethno-Nationalist groups have produced 17% of all injury cases. For all attributable major *and* minor cases, Religious groups have accounted for 69% of all injuries and Ethno-Nationalist groups are responsible for 16% of all injuries. (See Figure AI-13 & Figure AI-14.)

When examining fatalities only in attributable major attacks, the figures show Secular Utopian groups leading with 57% of all deaths. Religious groups accounted for 35% of all fatalities. Finally, Ethno-Nationalist groups have produced 7% of all fatalities caused by major attacks against CI. (See Figure AI-15.)

For all fatalities in attributable major *and* minor attacks, attacks by Secular Utopian groups similarly reflect the most fatalities, 44.5%, with Religious groups responsible for 31% of all fatalities. The Ethno-Nationalist groups accounted for 11% of all fatalities. (See Figure AI-16.)

When sub-categories of the perpetrator types are considered, it is clear that Islamist groups have the distinction of being the most lethal, causing an average of 12 deaths per attack. In terms of non-lethal casualty producing attacks, Islamist groups also top the list with Cults and Right-wing groups responsible for significant, yet far smaller, numbers of fatalities. (See Figure AI-17.)

Perpetrator Groups

Of all attacks against infrastructure, the Shining Path, the Euskadi ta Askatasuna (ETA), the Irish Republican Army (IRA), the Revolutionary Armed Forces of Colombia (FARC), the National Liberation Army (ELN), the Armenian Secret Army for the Liberation of Armenia (ASALA), the National Liberation Front of Corsica (FLNC), and the Red Army Faction (RAF) account for the greatest number of attacks. Of these groups, the Shining Path, the IRA, and the FARC are responsible for the highest number of major and minor attacks. (See Figure AI-18.)

Specific Groups and Casualties

Of those specific groups identified as most active in attacking CI—the IRA, the ETA, FARC, Shining Path, the ASALA, the FLNC, and the RAF—none has conducted a CI attack that has killed more than four people. However, when the analysis is expanded to include groups that have been less prolific in attacking CI, casualty rates are far higher. Here Al-Qa`ida is the most lethal with 435 [412] fatalities while the LTTE is second with 187.

Type of Attack/Delivery

The analysis of data for major attacks on CI reveals that various methods of bombing seem to be the preferred mode of assault. Of the 188 major attacks, about 112 were implemented using various types of bombing. However, as most of the bombing types were in the Unknown category, no useful analysis can be drawn about the prevalence of different types of bomb. Following bombings, sabotage was the next most preferred method for attacking CI seems to be employing sabotage tactics. About 22 attacks employed such strategies.

The data for both major and minor attacks indicates that almost 63% of incidents involved various types of bombing. About 9% of attacks used projectiles such as mortars and rocket propelled grenades.

[412] This figure excludes the attacks of September 11.

Region and Attack Method

Various types of bombing are the most favored type of attack in all regions, accounting for 62% of all attacks. Projectiles were the next favored means of attack in all regions, yet they accounted for 9% of attacks. In Europe, bombings alone accounted for 69% of all attacks. Interestingly, Molotov cocktails have been popular types of attacks in Europe accounting for 10% of attacks. Given the crudeness and limited effect of this weapon, most of these attacks can be considered to have had a minor effect on infrastructure. In the Middle East and North Africa region, bombings were used 66% of the time, and projectiles were used 17.5% of the time. In the Latin America and Caribbean region, bombings were used 63% of the time. Projectiles and Sniping/Shooting were the next important categories in this region accounting for 7.8% and 9% respectively.

A statistical model was created to determine whether a relationship exists between the attacks occurring in a region and the type of attack, the type of infrastructure attacked, and whether the attack employed suicide tactics or not. The statistical model utilized the data for all major and minor cases present in the database and concluded that a correlation exists between the terrorist incident in a region and the method of attack employed.[413]

Group Name and Attack Method

Of the specific groups identified earlier as the most prolific in attacking CI, only the FARC has preferred Sabotage and Siege and Hostage taking as a type of attack over bombings when attacking CI. This is consistent with known and recorded attacks by the FARC, most of which were against Oil/Gas infrastructure. The ETA has consistently favored using bombings and projectiles in their tactics. The Shining Path is recorded as using Sabotage and Combination tactics in their attacks in addition to bombings. The only type of attack the FLNC is recorded as having used are bombings. Apart from one isolated attack using Projectiles, the IRA has almost exclusively used Bombing as their preferred method of attack against CI.

Type of Attack/Delivery and Casualties

Not surprisingly, the type of attack visited upon CI has a direct bearing on the casualties that follow. Bombings (either of the Unknown or Vehicle type) account for 82% of all deaths, reflecting the efficacy of this means of attack for terrorists. If one excludes Combination attacks (which account for 13% of fatalities), all other types of attacks—Shooting, Grenades, Fire-bombings, Sabotage, etc.—account for only 7% of all deaths combined. (See Figure AI-19.) A somewhat analogous pattern emerges if all casualties, not just deaths, are reviewed. Bombings (either of the Unknown or Vehicle type) account for 75% of all casualties, while Combination and Other constitute 17%. Siege and Hostage Taking, Sabotage, Projectiles (grenades and mortars), and Shootings almost entirely account for what remains.

Preliminary statistical analysis of the major and minor cases in the database indicates that the number of casualties varies according to the type of attack used. However, the variation of fatalities, injuries, and casualties between different types of attack methods was not significant when the data for the Bhopal gas tragedy and the terrorist attacks on September 11, 2004 were excluded from the analysis.[414]

---

[413] Multiple Discriminant Analysis was used to evaluate the relationship between the type of infrastructure attacked, the type of attack, the suicide/non-suicide nature of attack and the region in which an incident occurred. See Figure 2 in Appendix III.
[414] A one-way ANOVA test was conducted between the types of attacks and the mean number of fatalities, casualties, and the injuries. See Figure 3 in Appendix III (The SPSS output indicates the test results after excluding the cases of the Bhopal chemical incident and the terrorist attacks on September 11, 2001 in the U.S.)

Casualties

The number of fatalities for terrorist attacks against critical infrastructure in total was 9,034. However, when the fatalities for the incidents in Bhopal, India, and the September 11 attacks (which account for 6,820 fatalities and skew the data significantly) have been removed, the total drops to 2,214. Fatalities were highest in the decade 1990-1999. The number of injuries follows a similar trend.

Until the 1980s, CI attacks that resulted in fatalities were exceptionally rare. Since that time, however, attacks have become far more lethal with 1998 being a crescendo of sorts with well over 1,000 deaths. Indeed, the 1990s was the most lethal decade known, far eclipsing all other decades. The current decade is on track to be less deadly that the 1990s by a factor of two, although if the casualties of September 11 are included the current decade would be the most lethal. (See Figure AI-20.) When one includes non-lethal casualties as well, a similar pattern emerges. Again the 1990s led all decades in casualties, reaching just under 11,000. The 1980s had fewer casualties by a factor of almost six.

Conclusions

Between the 1960s and today, the total number of attacks by sub-national groups against CI targets appears to have risen dramatically. Even if one acknowledges that these numbers may be corrupted somewhat by the relative paucity of information gathered during earlier decades, serious gaps in the existing databases that attempt to record terrorist attacks and incidents, and the increasingly extensive media coverage of terrorist incidents that has marked successive decades, several patterns clearly emerge from even the most cursory examination of CrITIC compiled by CNS for this project, three of which are reviewed below.

First, with regard to the general attack numbers, the total number of attacks on CI increased from only 42 in the decade of the 1960s to 116 in the 1970s to 471 in the 1980s. Significantly, it decreased to 308 in the 1990s and now stands at 131 for the first three and one half years of the new millennium. In short, there has been nearly a ten-fold increase in the total number of CI attacks from the decade of the 1960s to that of the 1990s. (See Figure 4.2.) This seems to suggest that violence-prone non-state actors have developed a growing interest in attacking CI over time, although the percentage of increases in CI attacks would have to be compared to the percentage of increases in the total number of terrorist attacks over the past four decades in order to determine whether that number is 1) a simple reflection of the overall increase in terrorist attacks, or 2) a strong indicator of increasing interest in attacking CI per se. The difficulty with this is the lack of comparable data on non-CI related incidents. In either event, the interest of terrorists in carrying out such attacks is scarcely likely to decline in the near future, especially given the growing attention paid by Western and international media to CI vulnerabilities.

Second, with regards to the type of infrastructure attacked and method of attack, of the attributable major CI attacks between 1933 and 2003, Oil/Gas, Power, and Public Service/Government Office facilities were targeted most frequently. As is discussed in more detail below, the Oil/Gas Infrastructure category also accounted for the most number of casualties from the CI attacked. However, when factoring in minor attacks against CI, Embassies/Consulates were targeted close to 50% of the time, incurring a negligible number of fatalities compared to other CI categories. In attacking CI, bombing has been the most favored method of attack, however, given that most of the bombing types are unknown additional investigation is required to more fully understand these numbers.

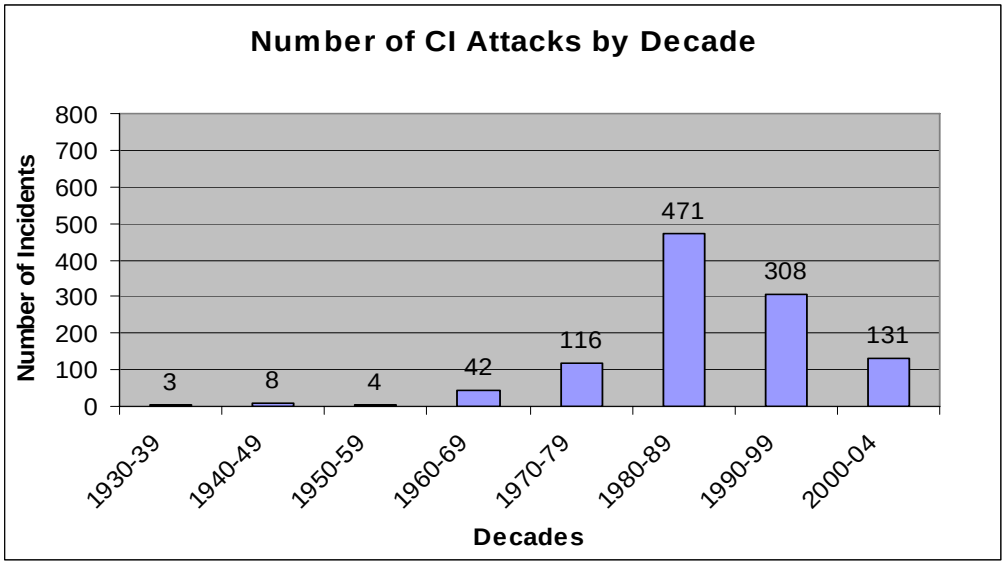


Figure 4.2

Third, apart from this extraordinary apparent increase in the number of CI attacks, which in part undoubtedly parallels the dramatic increase in the number of terrorist attacks of all types, there have also been noticeable shifts in the proportion of such attacks that have been carried out by different types of terrorist groups. Although the majority of the perpetrators of CI attacks in each decade fall into the "Unknown" category, of those that can be identified one discovers the following breakdowns. During the 1960s, the relatively small number of CI attacks were carried out by Ethno-Nationalist groups (8) and Secular Utopian groups (7). (Religious groups were only responsible for a single CI attack during this period.) From the 1970s onwards, it is notable that the number of CI attacks increase, and that those attacks in which the perpetrators are identifiable can be attributed mainly to Secular Utopian groups, Ethno-Nationalist groups, and Religious groups. Specifically, in the 1970s, Secular Utopian groups were responsible for 40 CI attacks, Ethno-Nationalist groups for 12, and Religious groups responsible for one attack. This same pattern generally holds true for the 1980s and 1990s, in which Secular Utopian groups were responsible for 161 and 62 CI attacks, respectively, whereas Ethno-Nationalist groups were responsible for 80 and 46, also respectively. However, during these two decades there was a significant increase in the number and percentage of CI attacks carried out by Religious groups compared to previous decades, 32 (7%) attacks in the 1980s and 31 (10%) in the 1990s. The trend in growing numbers of CI attacks conducted by Religious groups continues in the new millennium. Indeed, during the first three years of this decade, Religious groups have carried out 26 – or 20% of all CI attacks – comparable to the 30 (23%) conducted by Secular Utopian groups and surpassing the 11 (8%) conducted by Ethno-Nationalist groups. In other words, Religious groups are now among the most prolific in carrying out CI attacks.

If we break these general categories down further, it becomes clear that Left-Wing groups (above all Marxist-Leninist groups) carried out the overwhelming majority of attacks attributable to groups that fall within the Secular Utopian category, as opposed to Anarchist, Neo-Fascist, and Ecological groups. Similarly, Islamist groups were responsible for carrying out the majority of CI attacks that have been perpetrated by Religious groups in the past two decades. Between 1980 and 2004 Religious groups were responsible for 89 incidents of which, Islamist groups were responsible for 84 or 94% of the incidents. (See Figure 4.3.)

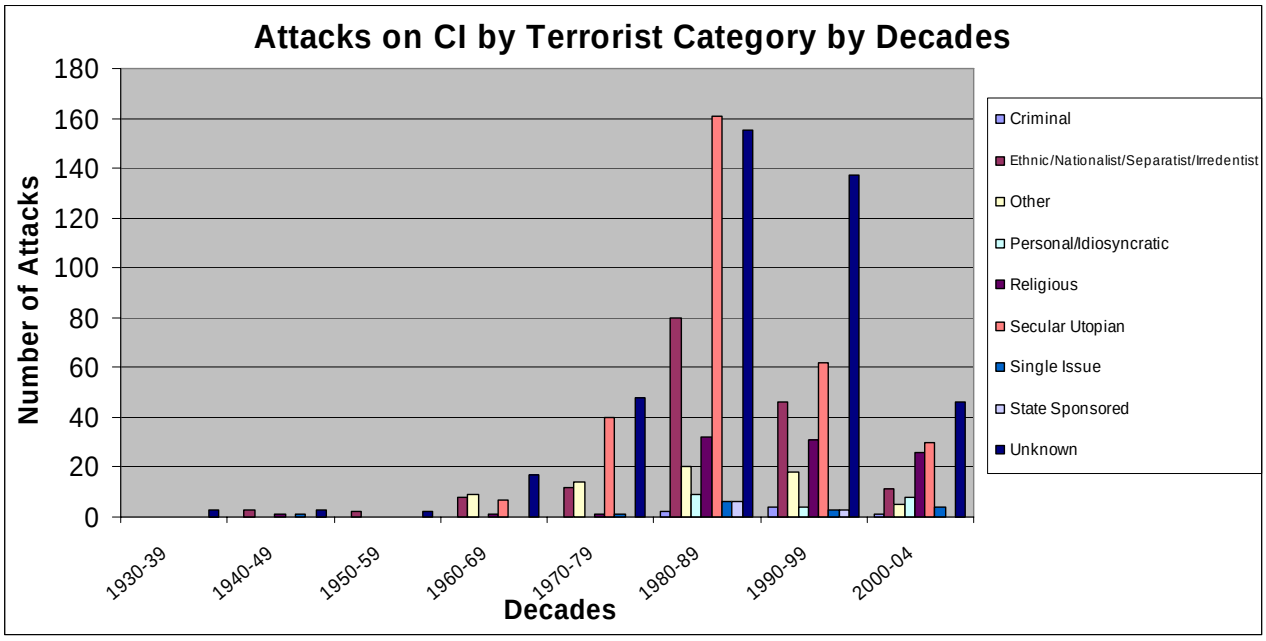


Figure 4.3

Finally, with regards to casualties, bombings have accounted for almost 80% of all CI attack deaths and 75% of all casualties when non-lethal injuries are included. Secular Utopian and Religious groups are the most deadly with the latter responsible for 80% of casualties of attributable major attacks and 35% of the fatalities in the same category. This seems to echo the trends seen in general in attacks involving religious terrorist groups. These statistics suggest a hypothesis proposing that religious groups are more likely than other groups to mix CI attacks with mass casualty attacks. In contrast, of the seven most active groups—the IRA, the ETA, FARC, Shining Path, the ASALA, the FLNC, and the RAF—none has killed more than four people in a single attack.

These, then, are the general patterns that emerge from the descriptive statistics generated from CNS's CrITIC. Time constraints limited the amount of data verification that could be done, as well as the number of statistical tests that could be run, and so all results are provisional. However, even a fairly cursory look at descriptive statistics yields more insight than has heretofore been available regarding attacks against critical infrastructure.

Chapter 5: THE DECIDe FRAMEWORK*

A. Introduction

There used to be a time in the not so distant past when a certain distance between conception and application was possible, even laudable. Scientists, both of the physical and social variety, could develop hypotheses at leisure, these hypotheses could be tested and refined over time to produce theories, and eventually, if they stood up to the scrutiny of peers and politicians, others would come along and engineer these theories into tools and products useful in daily life. Unfortunately, the devastating potential of contemporary terrorism and the urgency with which adequate tools to understand and counter terrorists are required make it untenable, in this domain at least, for theorists to sit back and wait for this orthodox progression. Basic research needs to be operationalized as soon as possible in a form that analysts, investigators and policymakers can deploy "in the field." It is with this in mind that an attempt is made here to combine the empirical research (both of the large *N* and case study varieties) on terrorist motivations for attacking critical infrastructure with the existing body of literature relating to terrorist target selection in order to produce a usable and useful analytical tool. Those fastidious about the scientific method will be quick to point out the inherent dangers in hasty execution. The current work is merely the first foray into analytical territory that has thus far been only cursorily explored, and it is eagerly anticipated that others will verify and build on our ideas. We feel that in this case, however, rigorous testing must not hold up assistance to those working in the trenches, where there is a dearth of analytical tools available in areas such as this one. Instead, we propose a synchronic, incremental approach, in which hypothesis, theory, and application remain linked, and as theory is refined, so too are the tools based upon that theory. We hope therefore that this will initiate an interactive discourse in order to constantly improve what is admittedly a preliminary tool. We have termed our construction the DECIDe (Determinants Effecting Critical Infrastructure Decisions) Framework and its goal is to assist in the assessment of whether a particular terrorist group is relatively more or less inclined to attack critical infrastructure as opposed to some other target.

A few words are necessary before delving into the framework itself. First, we do not call our construction a *model*[415] for the simple reason that many potential users of our tool in the policy and intelligence communities may already be wary of numerical models of terrorist thought processes. We have tried to avoid as far as possible anything resembling a mathematical formula or succinct algorithm[416] and firmly leave the ultimate conclusions in any particular case to the analysts themselves. Therefore, we prefer the term "analytical framework" and will refer to our construction as such.

Second, while the goal of much counterterrorism analysis is prediction, one must first gain a thorough understanding of the topic in question before reaching any predictive insight. The current framework – which is focused on terrorist decision making – is primarily descriptive in its orientation, with any predictive capability flowing from the descriptive aspect. This complicates matters somewhat in terms of the availability of methodological referents, in that many of the existing tools related to decision making were developed with the aim of optimizing the decision making process (in business, policymaking, and so forth) and are thus prescriptive[417] in nature and of little use in the current problem context.

---

* This chapter was written by Gary Ackerman.

[415] Even though, technically speaking, our tool falls into the *American Heritage Dictionary*'s definition of "a schematic description of a system, theory, or phenomenon that accounts for its known or inferred properties and may be used for further study of its characteristics."

[416] There may, however, be some superficial similarities in presentation.

[417] See, for example, the works of such authors as Ralph L. Keeney and Howard Raiffa, including, Keeny, R. and Raiffa, H. *Decisions With Multiple Objectives: Preferences and Value Trade-Offs* (Cambridge: Cambridge University Press, 1976).

Third, any useful framework must at the very least take into account the level of analysis problem inherent in decision making research. There has been much debate over the relative merits and shortcomings inherent in choosing between: 1) a 'systemic' approach in which terrorists' decisions are viewed primarily in terms of environmental constraints or stimuli and an initial set of variable values (which usually leads to some variant of a rational actor-expected utility approach);[418] 2) an 'organizational' approach that concentrates on group dynamics, power relationships and 'bureaucratic' influences; and 3) a 'psychological' approach that examines the biases and other distortions in decision making at the individual level. None of these approaches have been shown to be universally more successful over the others in describing terrorist decision making. It is one thing to say that terrorists attempt to maximize gains and reduce costs, just as all good rational decision makers do.[419] This is both true and deceptive, in that the determination of the benefits and costs, as perceived by the terrorist group, is the outstanding problem. Here, the devil, as they say, is certainly in the details. Models that focus on one level of analysis over the others are often successful in limited domains or when applied to certain terrorist groups at specific points in time. However, they are far from generalizable to all contexts, even though they are often portrayed as such, and can bias analysis. Our method does not adopt any dogmatic stance regarding the level of analysis and includes aspects from all three levels by having different factors influence ultimate decision outcomes.

Fourth, unlike the representations in several previous models of terrorist decision making, decisions often do not follow a strict succession (for instance, ideology => target selection => weapon selection) but can be more fluid in their ordering. Indeed, recent work in the cognitive sciences suggests that decisions are often the result of numerous mental processes occurring in parallel.[420] We have taken great pains to avoid falling into the trap of imposing a fixed process by creating a framework that is as flexible as possible and only ordinal where obviously and logically required. Moreover, in a real-world social context, decision making is a dynamic process with numerous opportunities for feedback. In the domain of terrorist target selection, this places the phenomenon of decision making – in the language of Snowden's *Cynefin* framework[421] – either in the realm of the "knowable" (since data may exist but often cannot be observed due to the clandestinity of terrorists) or the realm of the "complex" (owing to fundamentally unpredictable convergences of individual interactions) depending on the particular circumstances. As such, point prediction (based on the ideas of complexity science) may in many instances be theoretically impossible, and the correct strategy is to implement "probes" to explore the complex possibility space. Unlike Drake's target selection model,[422] which tends to be somewhat rigid and cybernetic, we have structured our framework to incorporate the above ideas by both allowing for bidirectional factor influences and remaining amenable to the generation of probes to explore those parts of terrorist decision making that are "unknowable."

---

[418] Even in this relatively 'simple' approach, there are usually serious data lacunae.

[419] See, for example, Bruce Schneier, *Secrets and Lies: Digital Security in the Networked World* (New York: Wiley Publishing, Inc., 2004), p. 43. "The rational adversary—not all adversaries are sane, but most are rational within their frames of reference—will choose an attack that gives him a good return on investment, considering his budget constraints: expertise, access, manpower, time, and risk. Some attacks require a lot of access but not much expertise: a car bomb, for example. Each adversary is going to have a set of attacks that is affordable to him, and a set of attacks that isn't. If the adversary is paying attention, he will choose the attack that minimizes his cost and maximizes his benefits."

[420] See the theory of conceptual blending in Fauconnier, Gilles and Turner, Mark. *The Way We Think* (New York: Basic Books, 2002).

[421] David Snowden, an innovator in the field of knowledge engineering, has developed the Cynefin framework, which places problems and issues in various domains (the 'known', the 'knowable', the 'complex' and the 'chaotic') and prescribes different strategies for dealing with elements in each domain. See Kurtz, C. F. and Snowden, D. J. "The New Dynamics of Strategy: Sense-making in a Complex and Complicated World", *IBM Systems Journal* Vol. 42, Number 3, (2003), accessed online on July 27, 2004 at http://www.findarticles.com/p/articles/mi_m0ISJ/is_3_42/ai_108049867.

[422] See C.J.M. Drake, *Terrorists' Target Selection* (New York: St. Martin's Press, Inc, 1998), p. 180.

Finally, having exposed ourselves to the vast majority of available open source data and literature on the topic, we have grown naturally mindful that other modeling approaches may be useful in addressing this critical issue. Given the relatively limited scope of this study, however, we are unable to pursue these methodologies in depth. Consequently, Appendix IV ("Possible Model Extensions") offers a vignette of other potentially promising threat modeling and assessment methods that merit further consideration as possible tools for understanding the nexus between terrorism and CI.

B. Contributing Factor Diagram

Our framework is based on a *contributing factors approach*[423] that lays out the various elements that comprise a terrorist group's targeting decision and indicates the major relationships and interplay between these factors, as well as the direct influences on target selection. This approach was preferred since, unlike the traditional flowchart, decision elements are not presented sequentially but merely indicate a contributing effect (or possible contributing effect) on other factors.[424] Although it may appear as if we are dividing up the elements of the decision making process into discrete factors, we realize that within decision makers' minds there are rarely such strict delineations between the various elements of decision making. Thus, while bearing in mind that these factors may in fact intersect and possess fuzzy borders, for the purposes of presentation it is more useful to depict them as separable and to link factors together, rather than end up with a "factor soup." The complete factor diagram that forms the basis of our framework is shown on the following page as Figure 5.1.

The most readily apparent quality of the factor diagram is that it is extremely complicated (some might argue needlessly so), but we feel that capturing the majority of the dynamics involved is more important than parsimony in this case. Part of the purpose of our framework is to make sense of these myriad factor influences so they can be used to reach a conclusion about the probability of a terrorist desiring to attack critical infrastructure.

The factors and subfactors used in the framework were arrived at as a result of a process of structured inquiry combined with a review of the literature, and have already been defined in Chapter 2. There may be differing opinions over whether a particular element should stand alone as a separate factor or whether it falls within the rubric of another factor and should serve as a subfactor. We do not argue that the construction we put forward is unique, or necessarily the most accurate representation of decision making. What is important, however, is that the structure is able to reflect the important dynamics and interactions involved in terrorist target selection and encompasses all levels of analysis. This is something we feel that our construction is capable of capturing. The various relationships between the factors are based upon a combination of information found in the literature, the results of our empirical research, and informed hypotheses, and are detailed as part of the framework discussion below.

Since most of the factors (at least those internal to the terrorist group) both influence and are influenced by numerous other factors, causation can, across different groups, and even with the same group under different circumstances, flow in either or both directions. For aesthetic purposes, we have endeavored where possible to situate "in" arrows entering at the top of each factor; "out" arrows originating from the bottom of each factor and bi-directional arrows at the side. Also, arrows can be linked to the overall factors themselves (i.e., indicating an influence on all aspects of the factor), in which case the arrows terminate at the factor box or in other cases arrows can be linked to specific subfactors.

---

[423] See Koller, Glenn, *Risk Modeling for Determining Value and Decision Making* (Boca Raton, FL: Chapman & Hall/CRC, 2000), although Koller's use of this approach to model terrorism is partial at best.

[424] Only the bottom-center portion of a diagrammatic representation of the DECIDe framework contains some degree of sequential ordering, reflecting the somewhat ordered final stages of the target selection process, viz. Primary Target Selection Surveillance and Assessment Decision to Attack Critical Infrastructure.

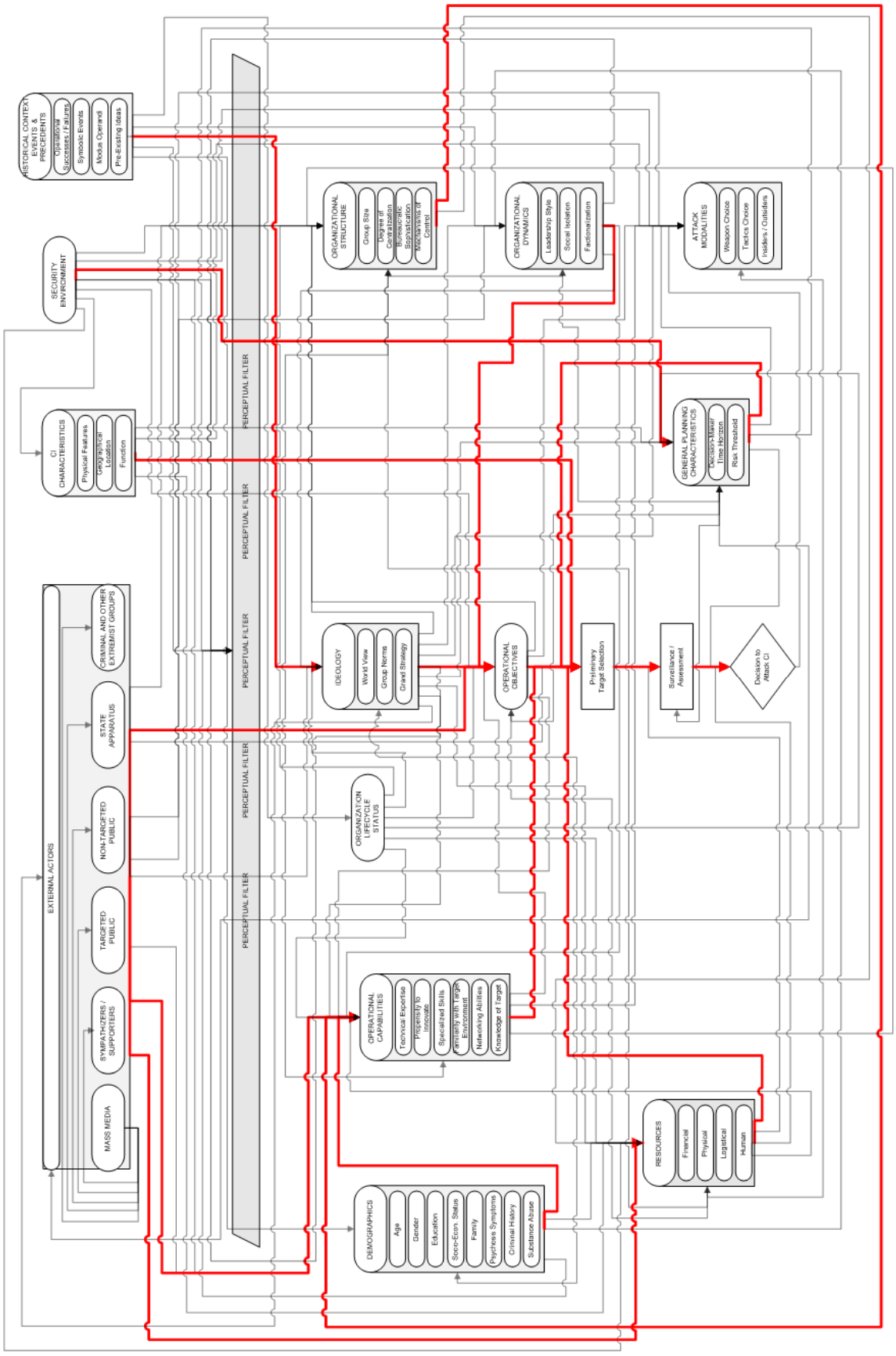


Figure 5.1: Contributing Factors Diagram

The Perceptual Filter differs somewhat from the other elements of the diagram in that it portrays both a factor and a *field*. While a factor in its own right that can be influenced by other factors, it serves two additional purposes. First, it graphically separates in a general way factors "internal" to the terrorist group from those "external" to the group,[425] and second it serves as a field that acts on information flowing in from certain external factors (which on the diagram pass THROUGH the perceptual filter instead of around it) to internal framework factors and indicates the possibility for perceptual distortions of information.

Although all the factors and relationships shown are considered in the framework, project researchers have indicated those relationships they feel to be most important in the majority of contexts by using a heavier line. However, we must caution that this simplification should not be relied upon because the varied, and often unique, nature of each terrorist group means that in certain cases a particular relationship that has minimal influence on decisions elsewhere plays a large role in a specific terrorist group at a specific time. Additionally, it should be noted that the framework often refers to terrorist groups or decision makers within groups. This does not detract from its utility in the specific case of an individual terrorist or a unitary decision maker. These should be viewed as examples of the more general case, and the framework is considerably simplified in these cases.

Two more preliminary notes should suffice to conclude the introduction to the DECIDe framework. The authors understand that terrorists do not base their decisions on a binary question: "do we attack a critical infrastructure target or something else?" Instead, terrorists will in all probability simply consider specific types of targets that may or may not fall within the critical infrastructure category as defined by academics and governments. Our primary focus of inquiry, however, is distinguishing target selection on the basis of whether the ultimate target selected by a terrorist group is one that is regarded as part of the nation's critical infrastructure, as well as the process by which such decisions are made. Therefore we have structured the framework on the basis of CI versus non-CI targets, even though we understand that each category is made up of many individual target types. The framework may in some cases reveal the specific type of critical infrastructure that could be attacked, but this is a corollary to the primary research question addressed by the framework.

As should be clear from the factor diagram, the DECIDe framework is dynamic in many respects, since influences on decisions can circulate through several factors and back again in the process of contributing to decision making. However, at this stage of the framework's development, the actual decision is regarded as single event focused and monadic. This means that the framework represents a 'one-shot' process – the group is considering a single attack, as opposed to a long-term campaign. Therefore, although the decision maker may take into account the reactions of external actors (such as the response of the public or the terrorists' constituency), these actors are not regarded at this stage as decision making entities in their own right, and their decision making processes are not captured in the framework. In order to accurately model a terrorist campaign, one needs to take into account the actual decisions made by external actors after each action perpetrated by the terrorists. This would require convoluted game-theoretic types of analysis and would only further complicate what is an already complex framework. The project team therefore decided to begin by considering an isolated attack process, which has the added benefit (from a simplification standpoint) of making several factors invariant under this single attack planning process.[426] Nonetheless, we feel that the framework presented here can still provide a powerful tool (and an improvement over existing methods) by capturing the most important dynamics of target selection, especially when considering terrorist groups with short planning horizons or "ad-hoc" groups that coalesce for the purposes of conducting a single attack, such as the group responsible for the first World Trade Center bombing in 1993.

---

[425] Since the entire diagram represents an internal decision making process, there are in actuality no external factors. However, to the extent that decision makers perceive items that exist in the external environment, these are here referred to as external factors for the sake of convenience.

[426] Further planned iterations of the framework will address these aspects of multiple actors and an added temporal dimension.

C. DECIDe Basics

The following is a general guide for using the framework, followed by the elements of the framework itself. The initial step in using the framework is trivial and is included here only for the sake of completeness. It must be stressed that this tool is designed to explore the intent of a terrorist group (or other violent non-state actor) to attack critical infrastructure; the other parts of a complete threat assessment (enemy capability and asset vulnerability) require different analytical tools. [427]

The DECIDe framework operates through two separate mechanisms:

a) Detecting increases in the relative attractiveness of critical infrastructure targets to the terrorist group and its perceived capability to attack these targets.

Within the framework, A is used to denote the attractiveness to the group of attacking a critical infrastructure target and C to denote the terrorist's perceived capability to engage in a serious attack against critical infrastructure targets. Increases or decreases are represented by '+' and '–' signs as follows:

Some increase	:	+	Some decrease	:	–
Significant increase	:	++	Significant decrease	:	– –
Large increase	:	+++	Large decrease	:	– – –
Varying increase	:	+ …	Varying decrease	:	– …
(dependent on characteristics of the variable)			*(dependent on characteristics of the variable)*		

The analysis begins with both A and C neutral.

b) Identifying progressive restrictions on the target space available to terrorists.

Following the lead of Drake and others it is possible to elucidate a mechanism by which one looks at the entire range of feasible targets open to terrorist attack, and then uses knowledge about the group's preferences and abilities to progressively restrict the set of targets that the group can or would attack. This approach supplements (a) the above in that it creates boundaries between the probable and improbable target sets. We regard (a) as a bottom-up approach in that it traces the individual factors that increase or decrease the motivation and perceived capability specifically to attack critical infrastructure. Yet the danger here is that the analyst will "fail to see the forest for the trees," so to speak, and could become so enmeshed in details that obvious limitations on the terrorist's freedom of target selection are overlooked. In that respect, this "top-down" approach provides a valuable check on (a) by progressively limiting the decision space. There is, however, an obvious limitation to using this second approach in isolation. While it can help verify whether or not critical infrastructure targets fall within the feasible attack space, it does not speak to the factors that may draw terrorists to critical infrastructure in particular. A combination of the two approaches therefore results in an accumulation of attractors towards critical infrastructure attacks on the one hand (through (a)), and a circumscription of targeting options on the other (through (b)), thus yielding mutually supportive analysis.

[427] Capability and vulnerability are therefore only important in so much as they affect motivations. We are primarily interested in terrorists' *perceptions* of their capabilities and target vulnerability, even if these differ considerably from the objective values of these variables.

In the most general sense, perhaps the best way to depict the process of target selection is as a series of concentric circles. (See Figure 5.2). A terrorist group's ideology establishes the boundaries of the largest and most all-encompassing of these circles, since it essentially identifies the full range of targets that can legitimately be attacked. Within that range, which is normally quite wide, a group's specific operational objectives for carrying out an attack will then necessarily lead to further reductions in the scope of targeting possibilities. Once the boundaries of all of the targets that might permit the group to accomplish its particular objectives are drawn, the group's existing level of operational capabilities will then likely impose further limitations on the number of potential targets which can reasonably be expected to be attacked successfully. At that point preliminary surveillance of those remaining targets is typically undertaken in order to determine precisely which ones are most vulnerable to attack. After this surveillance process has been completed, a final target is normally selected, and operational planning then begins in earnest.[428]

Owing to the paucity of literature or information pertaining to several areas of the framework, it was decided to include author hypotheses. These hypotheses were derived from the extensive experience and empirical knowledge of team members with the subject matter. While investigating and verifying extant hypotheses is a necessary and urgent task, it is beyond the scope of the current project. At the very least, these hypotheses provide fodder for future research efforts, and various approaches that may prove useful in this regard are described at the end of this chapter.

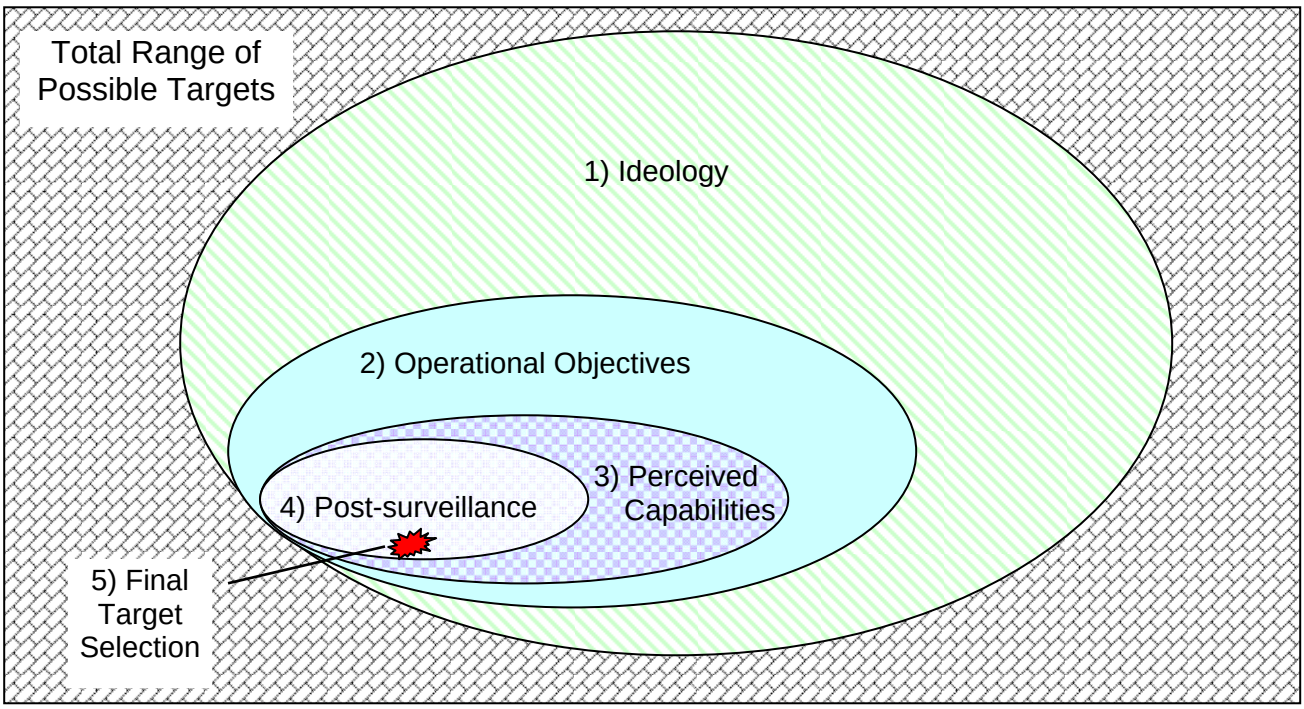


Figure 5.2: Progressive Restriction of Target Space

[428] Cf. the testimony of an American left-wing radical who specialized in bombings, cited in Bruce Hoffman, "Modern Terrorist Mindset: Tactics, Targets, and Technologies," The Center for the Study of Terrorism and Political Violence, (October 1997), pp. 13-14.

Instructions for Using the Framework

The section begins by broadly describing each of the four steps. It then provides an in-depth "walk-through" of the entire process.

Step 1: Preliminary Investigation

The first step involves investigating whether there are any overt or covert signs that the group possesses the intent to launch a serious attack against critical infrastructure. If so, the analysis terminates with a presumption of intent.

Step 2: Data Collection

The framework is almost entirely data driven, so the next step is for analysts to collect as much general data on the group and its environment as possible. A list of questions useful to the framework is contained in Figure V-3. Of course, it is highly unlikely that the answers to all, or even most, of these questions will be available (at least in the time frame available to most analysts). However, the more questions that can be answered and the greater detail with which these answers can be given, the fewer inferences will be necessary and the greater the utility of the framework will be.

The framework can be used by analysts working in both the open and classified realms – all that differs is access to data sources. Examples of sources that whenever possible should be consulted are given below:

***Unclassified*:**

- manifestos, communiqués and other publications produced by the group to communicate to their perceived constituency;
- interviews given by group members;
- internal group documents that have become public;
- court transcripts (including witness testimony and prosecution evidence);
- scholarly work;
- news reports;
- personal interviews with experts and investigative journalists

***Classified*:**

- visual surveillance;
- communications intercepts;
- prisoner interrogation;
- reliable informant reports;
- confiscated materials (documents, computer files, etc.)

An integral part of this step is obviously a determination by the analyst of the credibility of sources and evidence, but this is a separate topic beyond the scope of this paper.

Step 3: Factor Analysis

It is at this stage that the data is applied to the framework. Each factor[429] is considered in turn[430] and makes a specific contribution to the final determination of intent regarding target selection. The order in which analysts undertake this is largely unimportant, so long as the result of analyzing each factor is noted. In order to assist DECIDe users to keep track of their analysis, a worksheet has been provided (Appendix II).

The following procedure is followed for EACH factor:

a) The analysis of each factor begins with a list of the data requirements that need to be met to complete the analysis of that factor. These requirements are drawn from the master list of questions discussed in Step 2. Where information is available, it should be included. If all the requirements are met, analysts can proceed directly to step c) below.
b) Where the required information is unavailable, analysts then proceed to the Factor Influences List for the current factor, which details all the influences on the current factor that this study has been able to discern.[431] After reading and considering these influences, analysts can combine these guidelines with the broader data set regarding the group (collected in Step 2) and their existing knowledge base and produce inferences about the unanswered questions.[432]

   Illustrative example: In considering the resources factor, I need to find information on the group's level of financial resources. This information is unavailable, so I proceed to the Factor Influences List: Resources. After reading this list, I note that groups that have state sponsors usually have relatively high financial resources available. Since I know from my general research of the group that this group has a state sponsor, I can infer that their financial resources are considerable.

c) Once an answer or inference has been obtained for as many of the listed questions as possible, analysts can proceed to the "flowchart" section of the factor analysis. The flowchart section supplies guidance for proceeding, depending on the data. For example, the flowchart might recommend increasing or decreasing A or C, restarting the analysis under different initial conditions or limiting the target space. The flowcharts have been produced using a combination of the results in Chapters 2, 3 and 4, and will only be annotated where results are particularly speculative or counterintuitive.
d) The analyst should record on the worksheet any changes suggested by the analysis of that factor and move on to the next factor.

Step 4: Determination of Intent

Once the factor analysis has been completed and all (or most) of the factors besides the Operational Objectives and Target Selection Process (consisting of Preliminary Target Selection, Surveillance and Final Target Selection) have been considered, the analyst should move to the Determination of Intent step of the framework where the various factor influences are combined and the target space evaluated to arrive at a determination of the existence and strength of the group's motivation to attack a critical infrastructure target.

---

[429] Factors that have no *direct* influence on target selection and are not influenced by other factors in the model do not need to appear in the factor analysis (although relevant data requirements relating to these factors still appear in the Master Data Requirements List and should be answered if possible). The factors thus excluded are: Security Environment, Organizational Life Cycle, and Historical Events.

[430] Where time for analysis is truncated, analysts may want to concentrate on the factors for which the most data is available, although this can lead to an underestimation of vital determinants of decision making and should be avoided wherever possible. Also, the Operational Objectives and Target Selection sections cannot be excluded.

[431] These correspond with the connecting lines in the factor diagram. Hypotheses are noted in red and are italicized, giving analysts the choice to include or discard them from the analysis. Although all possible factor relationships were considered, where no significant or direct relationship was identified or hypothesized, these factors are excluded from the factor influence list in order to conserve space.

[432] The analysis can in fact resemble an inferential jigsaw puzzle, since inferences arrived at later on in the process can actually be used to address some unanswered questions associated with factors considered previously.

We do not claim that our framework leads to a 'correct' answer, or even to a unique one. The final determination is very much dependent on the analyst's expertise and different analysts may well reach differing conclusions. We feel that this is a strength rather than a weakness of our approach – we do not seek to replace analysis, which is both an art and science, with formulaic expressions based on arbitrary quantifications. Many analysts probably already follow similar frameworks to DECIDe, albeit usually intuitively. Intuitive analyses, however, hold several shortcomings. Among these are the lack of transparency (often even to the analyst herself, who may process many elements unconsciously), which can obstruct acceptance and adoption of the analysis by other parties such as policymakers, and also the imperfect information-processing capabilities inherent to any human being, which often result in a variety of biases[433] and, occasionally, glaring analytical omissions. We present a tool here that encourages the basing of analysis on available theory and empirical evidence,[434] as well as transparency about assumptions and evidence. It also enables the simultaneous consideration of multiple influences on the target selection process, something that is quite difficult using traditional analytical approaches.

[433] Terrorists are hardly the only actors prone to the perceptual distortions described in Chapter 2.

[434] As discussed in Chapter 1, the following scheme is used to categorize evidence types within in the DECIDe Framework: the following scheme is used to characterize assertions derived from the literature:

- 1 – Primary author assertion only
- 2 – Multiple authors' assertion
- 3 – Anecdotal evidence
- 4 – Theoretical evidence (e.g. derived from a game theoretic model or clinical study)
- 5 – Large *N* Study (based on statistical data)

The highest degree of evidence present in each case is annotated.

Step 1: Preliminary Investigation

Data Requirements:

- Is there evidence that the group is planning to attack critical infrastructure in the short to medium term? This could include a communiqué expressly announcing such intentions or intelligence (from an informant, intercepted signal etc.) indicating active planning to attack critical infrastructure.

- Has the group attacked or made serious attempts to attack critical infrastructure in the recent past?

If the answer to either of these questions is affirmative, there is a presumption of intent, and the rest of the framework becomes unnecessary.

In the majority of cases, however, there will be no direct evidence indicating the intent to attack critical infrastructure; in fact, one of the difficulties of counterterrorism is that often little is known about a group's planning beyond "they are dangerous and want to hurt us."

This then leads us to the next step.

Step 2: Data Collection

Master Data Requirements List

1. How long has the group existed in its current form (i.e. as a separate organization)?
2. How many generations of members has the group had?
3. What is the observed ideology of the group (including worldview, grand strategic aims and the nature of the perceived enemy)?
4. What is the group's attitude towards human casualties?
5. Which historic events hold symbolic relevance for the group?
6. Is there any evidence of a specific dominant operational objective?
7. What is the size of the group (active members)?
8. Is the organizational structure more centralized (collected in a single geographic region) or more diffuse (for instance, cells scattered over several countries)?
9. Who makes targeting decisions in the group? (autocratic single leader, consultative council, sub-commanders etc.)
10. Does the decision making style tend to be autocratic or consensual?
11. To what extent are leadership decisions carried out?
12. What is the status and position of various factions within the group?
13. What are the demographic characteristics of key group decision makers, especially in terms of education, vocation, and family background?
14. Do any key group decision makers exhibit clear symptoms of psychopathologies that could lead to perceptual impairment?
15. Is there evidence that group decision makers habitually exhibit particular cognitive or affect-based biases? If so, which biases dominate and how do these tend to manifest?
16. What is the general level of the group's financial resources?
17. How stable/dependable are current sources of financial resources and what is the cost to the group to obtain them?
18. What kinds and amounts of physical resources (weapons, equipment, vehicles, etc.) does the group possess?
19. How expansive and sophisticated is the group's logistical infrastructure?
    a. Do they have access to safehouses, secure communications, travel documents and so forth?
    b. What amount of redundancy is built into the logistics system?
20. What type of security environment does the group face at the time of target selection?
21. How vulnerable is the group to detection, infiltration and elimination by the security forces of their opponents?
22. Do group decision makers have a set timetable for action?
23. Does the group currently perceive itself to be under threat?
24. What is the group's history of innovation (both tactically and technically)?
25. What is the group's general technological level?
26. What is the group's knowledge level of various critical infrastructure targets (e.g. through an insider at a nuclear power plant, or someone trained as a roadway engineer)?
27. How familiar is the group with the general target environment?
28. Which external groups or organizations do the terrorist decision makers perceive as allies or potential allies?
    a. Of these, the support of which external groups or organizations do they seek to gain or maintain?
29. Which external groups do the terrorist decision makers perceive as opponents?
30. What is the level of publicity terrorists expect from different media groupings?
31. What does the group perceive the functionality of various targets to be and the consequences they expect from a successful attack against a target that falls within the CI category?
32. How has the media recently portrayed critical infrastructure?
33. What is the level of protection decision makers perceive CI targets in general (relative to other targets) or particular CI targets of interest, to have?
34. What is the level of publicity they expect to receive by attacking various targets?
35. How tolerant are decision makers about risk (in terms of operational success, group survivability and the welfare of group members)?

Step 3: Factor Analysis

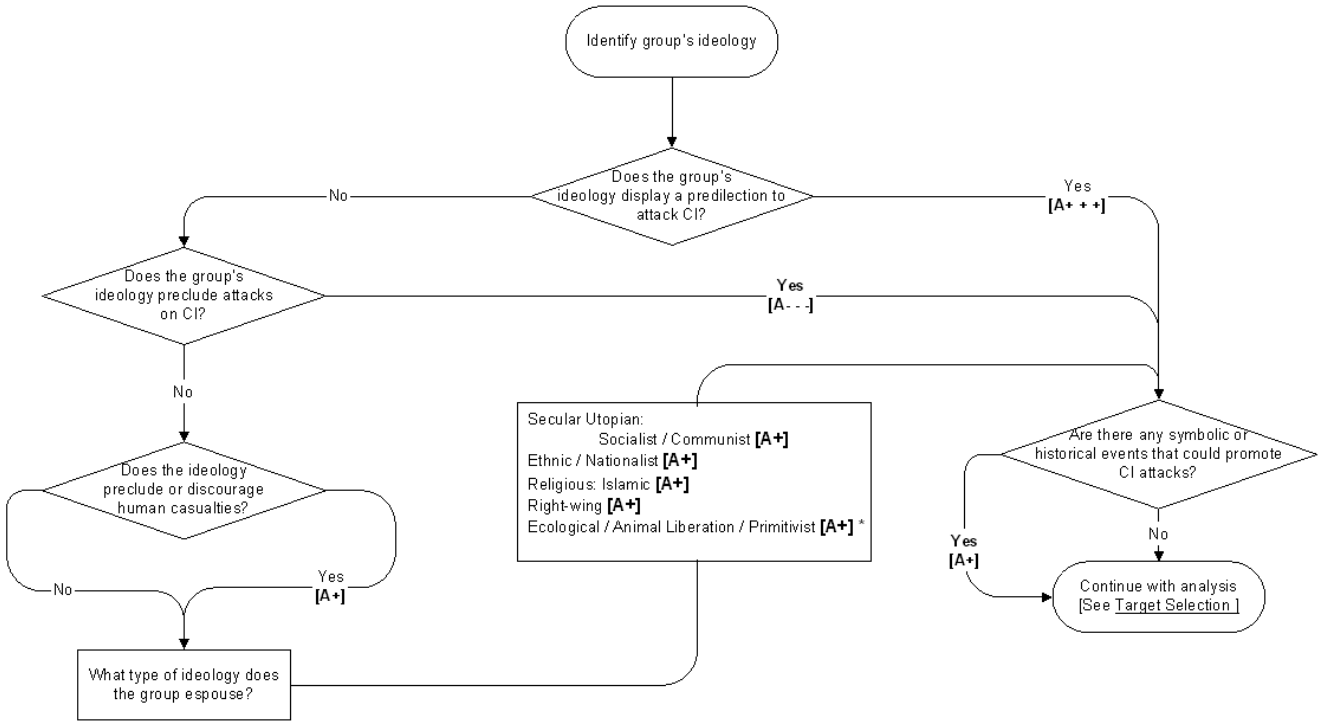
Factor Analysis: Ideology

Data Requirements:

- What is the observed ideology of the group (including worldview, grand strategic aims and the nature of the perceived enemy)?
- What is the group's attitude towards human casualties?
- Which historic events hold symbolic relevance for the group?

[This factor is relatively invariant DURING the decision making process]

If data exists for the above questions, proceed to flowchart. Otherwise, derive inferences from Factor Influences List (following page) and then return to the flowchart.



* This box is derived from results contained in Chapters 2, 3 and 4, and is shown in the context of attacks in the United States.

Factor Influence List: Ideology

Organizational Dynamics affecting Ideology

- There is no evidence in the literature surveyed to indicate that organizational dynamics impacts ideology.
- *Hypothesis: Breakaway factions from terrorist groups are generally more ideologically radical (and thus are also often more prone to violence) than their parent organizations.*

Demographics affecting Ideology

- According to Hoffman, the underlying focal point of terrorism is action and, even more, "the thrill and heady excitement that accompanies it." This implies that underlying psychological needs – in this case a craving for excitement – precede and condition ideological rationales.[435] [Evidence Type: 3]
- *Hypothesis: In cases where decision making is dominated by a psychopathic or sociopathic personality, there is a smaller probability of constraints on causing multiple casualties.*
- *Hypothesis: Education may influence ideology in that groups whose key members are better educated are likely to espouse more sophisticated doctrines.*
- *Hypothesis: Education is likely to affect ideology in that members of terrorist groups have either been inculcated with the dominant world views in their own societies or are consciously rebelling against them. For example, in parts of the world where religious instruction is included as an integral part of the educational curriculum, this may be a key source, implicitly or explicitly, of the ideology of members of terrorist groups.*

External Relations affecting Ideology

- For nationalist and separatist groups, Cameron argues that since the support of a "natural constituency" is crucial for them, they are "much more likely to be moderate in their actions because that support is conditional."[436] The implication is that such groups are less likely to resort to extreme violence and indiscriminate targeting. [Evidence type: 1]
- Parachini notes that societal alienation was a factor in shaping the worldviews of the perpetrators of several mass casualty incidents, and that their very alienation from society was in part responsible for the fact that they were not constrained by the usual societal norms against violence. [437] [Evidence Type: 3]
- Those terrorist groups that rely heavily (either ideologically or logistically) on external support - especially from sympathizers or a perceived constituency such as the general public, but also from other criminal/extremist groups, etc. - will usually (but not always) limit their violent actions to what these external groups will find tolerable. They will at least take the impact of their actions on outside groups into account when deciding upon their operational objectives.[438] [Evidence Type: 1]

Historical Events affecting Ideology

- McCormick argues that historical precedents, including prior practices – which he characterizes as "the (interpreted) experiences of…predecessors" – serve as "attractive guides" for terrorist action.[439] [Evidence Type: 2]

Perceptual Filter affecting Ideology

- The perceptual filter is not only affected by a group's ideology, but can exert a reciprocal, although often more subtle, influence on a group's ideology. In this case, the constant framing of incoming information usually serves to reinforce and intensify existing ideological beliefs in that counterfactual information is mostly excluded or distorted to reflect existing beliefs about good and evil, the nature of the enemy and the righteousness of the group's ultimate goals. Depending on the strength of the perceptual filter (determined *inter alia* by the structural control of information to and within the group and the degree of social isolation of group members), this can lead to a vicious cycle in which existing beliefs influence the interpretation of outside events, which in turn further entrench or exacerbate these beliefs.

---

[435] Bruce Hoffman, "The Modern Terrorist Mindset: Tactics, Targets, and Technologies," The Center for the Study of Terrorism and Political Violence, St. Andrews University, Scotland (October 1997), p. 12.

[436] Gavin Cameron, "*Nuclear Terrorism: A Threat Assessment for the 21st Century*" (New York: St. Martin's Press, 1999), p. 159.

[437] John Parachini, "Comparing Motives and Outcomes of Mass Casualty Terrorism Involving Conventional and Unconventional Weapons," *Studies in Conflict and Terrorism*, No. 24 (2001), p. 397.

[438] Cameron, *Nuclear Terrorism*, pp. 156-157.

[439] Gordon H. McCormick, "Terrorist Decision Making," *Annual Reviews in Political Science* 6, (2003), p. 488.

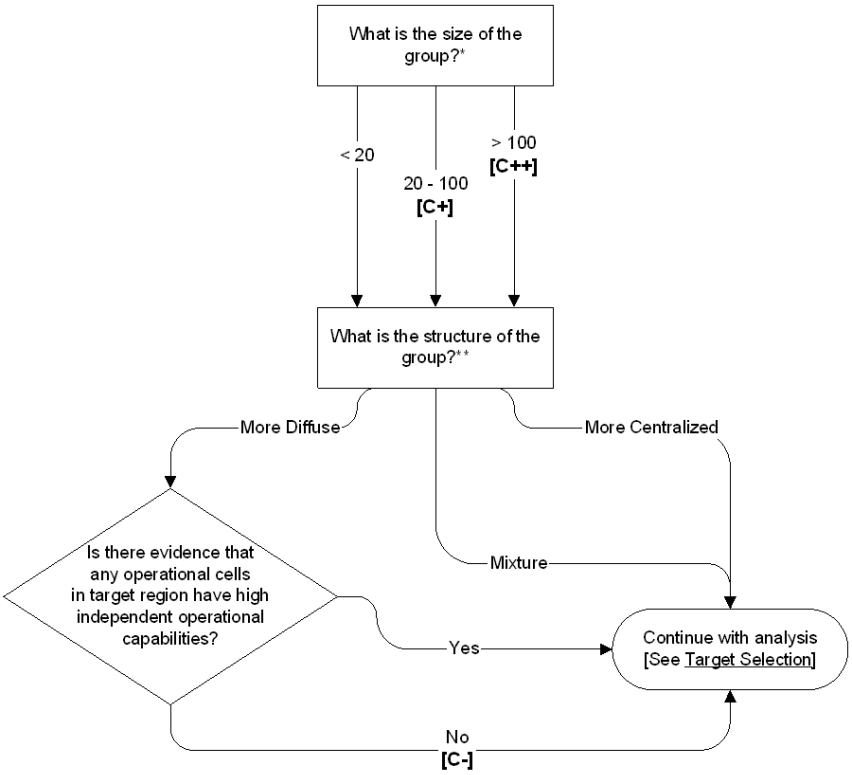
Factor Analysis: Organizational Structure

Data Requirements:

- What is the size of the group (active members)?
- Is the organizational structure more centralized (in a single geographic region, for example) or more diffuse (perhaps as scattered cells scattered)?

[This factor is relatively invariant DURING the decision making process]

If data exists for the above questions, proceed to flowchart. Otherwise, derive inferences from Factor Influences List (following page) and then return to the flowchart.



* Drake states that a group's size affects its targeting strategy. Specifically he argues that larger organizations with more members can carry out more attacks, including ones against less prominent targets (and they perceive this).[440] [Evidence Type: 3] Drake also suggests that organization size can impact a group's knowledge of targets. Specifically, larger groups will have the manpower to collect more information about potential targets, enhancing their ability to select good targets that can be effectively attacked.[441] [Evidence Type: 1]

** *Hypothesis: There are benefits that result from a centralized structure, in terms of organizational learning and exploitation of specialization opportunities. A cell isolated from the main group will be unable to leverage any of these benefits and, unless its members have been specifically selected for their expertise or have other capabilities independent of the parent organization, it can be expected to experience a diminution in overall capabilities over time. This may be more than offset, however, by the benefits of a diffuse structure, such as the increased ability to avoid detection by security forces.*

[440] C.J.M. Drake, *Terrorists' Target Selection* (New York: St. Martin's Press, Inc, 1998), p. 80.

[441] *Ibid*.

Factor Influence List: Organizational Structure

General

- Drake states that group size directly affects the formality of a terrorist organization's internal structure. Specifically, small groups are more likely to operate with loose, informal structures. Larger groups, however, are more likely to develop formal bureaucratic structures.[442] [Evidence Type: 1]
- Drake also suggests that group geography also influences an organization's structure. A group that has members that live close together is more likely to be able to operate efficiently with a less organized bureaucracy, than one that has its members spread over a wider area.[443] [Evidence Type: 1]

Ideology affecting Organizational Structure:

- There is no evidence in the literature surveyed to indicate that ideology impacts organizational structure.
- *Hypothesis: Ideology may well affect a particular terrorist group's organizational structure, e.g., groups with radically anti-authoritarian political agendas are arguably likely to adopt less authoritarian, centralized, and hierarchical organizations.*

Organizational Dynamics affecting Organizational Structure

- Post comments that leadership style affects the structure of a terrorist organization. Leaders with authoritarian, charismatic, narcissistic, paranoid and totalitarian personalities – in particular – are presented as types of individuals who will seek to create situations in which they can exert strong central control over their organizations (i.e. higher centralization).[444] [Evidence Type: 2/4]

Operational Capabilities affecting Organizational Structure

- Sinai alludes to the fact that terrorist organizations' operational capabilities may influence their structure. Specifically, as the technical capabilities of a terrorist group become increasingly specialized and sophisticated, its organizational structure may become increasingly diversified and compartmentalized into specialist units (i.e. elements that work with finances, recruitment, public relations, military operations, etc.).[445] [Evidence Type: 3]

External Relations affecting Organizational Structure:

- Silke points out that there is an influence on the Organizational Structure of a group when there is a sympathetic or supporting group involved, as evidenced by internal rules designed to foster and maintain support among what are seen as constituents.[446] [Evidence Type: 1]

Security Environment affecting Organizational Structure

- Muller suggests that the security environment may influence groups' tendencies toward hierarchical and command-oriented structures – the harsher a security environment the more centralized decision-making is likely to become to maximize offensive capabilities and survival. (Note this does not preclude the use of cells for security purposes.)[447] [Evidence Type: 1]

---

[442] Drake, *Terrorists' Target Selection*, p.77.

[443] *Ibid*.

[444] Jerrold M. Post, Keven G. Ruby, and Eric D. Shaw, "The Radical Group in Context: An Integrated Framework for the Analysis of Group Risk for Terrorism," *Studies in Conflict and Terrorism*, 25 (2002), p. 85-88.

[445] Joshua Sinai, "Analytical Model of Terrorism Forecasting," International Conference on Post Modern Terrorism, September 2003.

[446] Andrew Silke, "Beating the Water: The Terrorist Search for Power, Control, and Authority," *Terrorism and Political Violence*, 12:2 (Summer 2000), p. 77.

[447] Harald Muller, "Terrorism, proliferation: a European threat assessment," Institute for Security Studies, *Chaillot Papers* #58 (March 2003), p. 34-35.

Life-Cycle affecting Organizational Structure

- Thomas and Jackson[448] suggest that terrorist organizations progress through certain "life-cycles." The maturity of an organization, therefore, affects shifts in "internal functions" and "decision-making." Although Thomas[449] identifies this as a process, he doesn't provide specific examples of how the life-cycle impacts structure. Jackson suggests that older organizations become increasingly complex and have time to develop larger, more extensive and complex networks. [Evidence Type: 2]

Operational Objectives affecting Organizational Structure

- *Hypothesis: operational objectives can influence the long-term structure of an organization, especially if these objectives prescribe a sophisticated operation. In such a case, a group's structure might become increasingly specialized in order to meet the needs of a complex operation. This would only make sense for the group under a single attack planning process, if the operation is large, complex and will have high-impact effects.*

[448] Brian A. Jackson, "Technology Acquisition By Terrorist Groups: Threat Assessment Informed by Lessons from Private Sector Technology Adoption," *Studies in Conflict and Terrorism*, 24 (2001), p.202.

[449] Troy S. Thomas, Maj., USAF and William D. Casebeer, Maj., USAF, "Violent Non-State Actors: Countering Dynamic Systems," *Strategic Insights*, 3:3 (March 2004), p. 1-2.

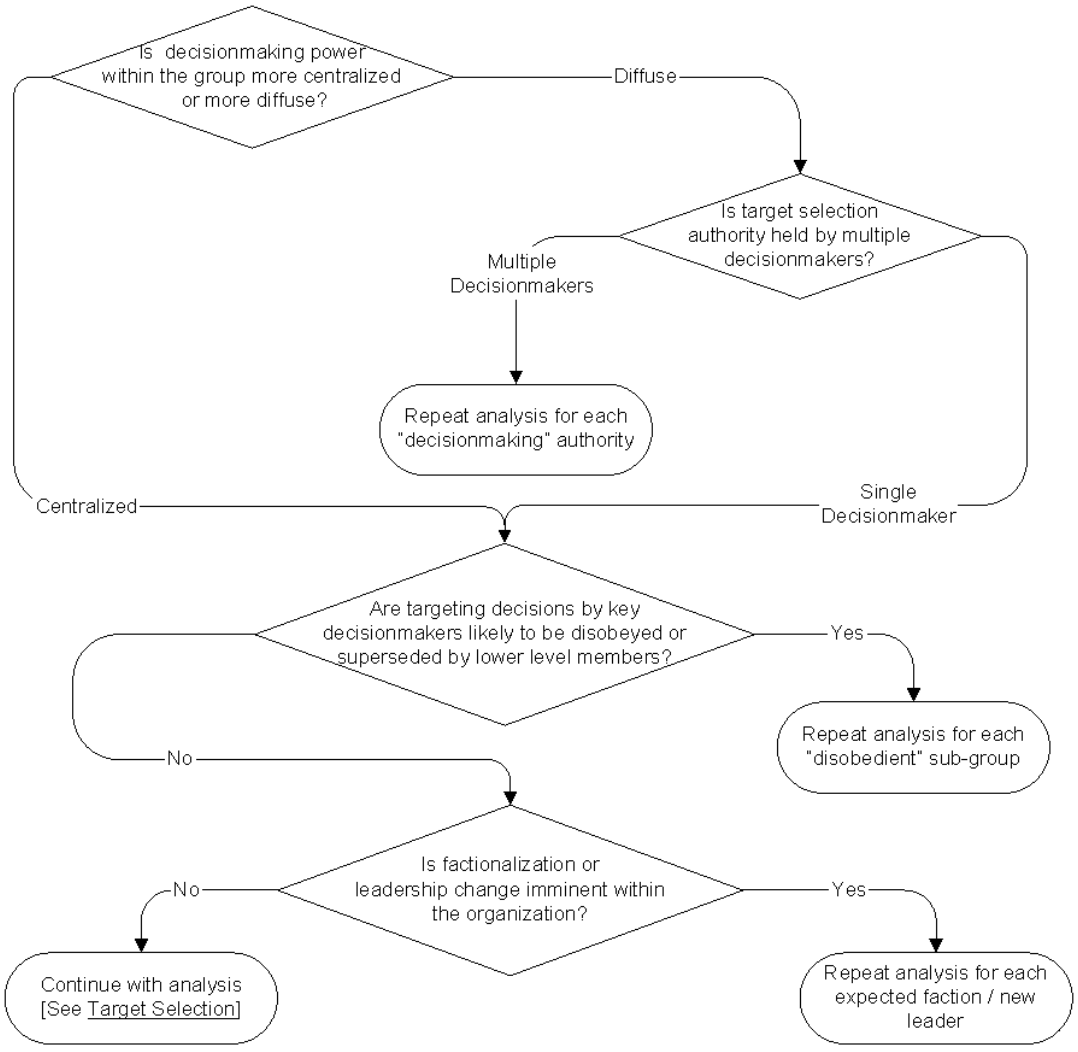
Factor Analysis: Organizational Dynamics

Data Requirements:

- Who makes targeting decisions in the group? (autocratic single leader, consultative council, sub-commanders etc.?)
- Does the decision making style tend to be autocratic or consensual?
- To what extent are leadership decisions carried out?
- What is the status and position of various factions within the group?

[This factor is relatively invariant DURING the decision making process]

Note: Organizational dynamics, while important in many areas of terrorist study, have very little direct impact on analyzing target selection, and even less impact on the decision between a CI and non-CI target. Organizational dynamics are, however, extremely relevant in determining the structure of the analysis. If data exists for the above questions, proceed to flowchart. Otherwise, derive inferences from Factor Influences List (following page) and return to the flowchart.



Factor Influence List: Organizational Dynamics

Historical Events affecting Organizational Dynamics

- McCormick suggests that historical events set the stage for the development of certain internal group dynamics. Specifically, he notes that the "frustration-aggression" hypothesis posits that a group's move toward violence can often be the result of a discrepancy between expectations and achievement.[450] [Evidence Type: 2]

Ideology affecting Organizational Dynamics

- There is no evidence in the literature surveyed to indicate that ideology impacts organizational dynamics.
- *Hypothesis: Whenever terrorist groups alter aspects of their doctrines, methods or objectives, this almost always leads to a process of factionalization or internal schism. Since many organizations undergo schisms or break apart after adopting even relatively small doctrinal changes, it may well be that an unpopular ideological shift will contribute to the dissolution of an organization.*

Demographics affecting Organizational Dynamics

- McCormick suggests that various ideological, social and demographic factors, including access to family and friends, social cohesion, costs of internal defiance, and the ability to leave the group, affect the internal dynamics of a group. Specifically, the more closely bound by common demographic factors and the more insular a group, the more likely its members are to act cooperatively.[451] [Evidence Type: 2]
- *Hypothesis: In terms of psychological health, clinically unstable decision makers (such as sociopathic personalities) may be less likely to be bound by ideological and other constraints and more likely to have punitive objectives.*

External Relations affecting Organizational Dynamics

- Silke points out that there is an influence on the organizational dynamics of a group when there is a sympathetic or supporting group involved, as evidenced by internal rules designed to foster and maintain support among what are seen as constituents.[452] [Evidence Type: 1]

General Planning Characteristics affecting Organizational Dynamics

- *Hypothesis: A short perceived time horizon (brought about, for instance, by an increasingly oppressive security environment) can result in increased stress levels that can have an impact on group dynamics.*

---

[450] McCormick, "Terrorist Decision Making," p. 491.

[451] *Ibid*, p. 491.

[452] Silke, "Beating the Water," p. 77.

▪ Factor Analysis: Demographics

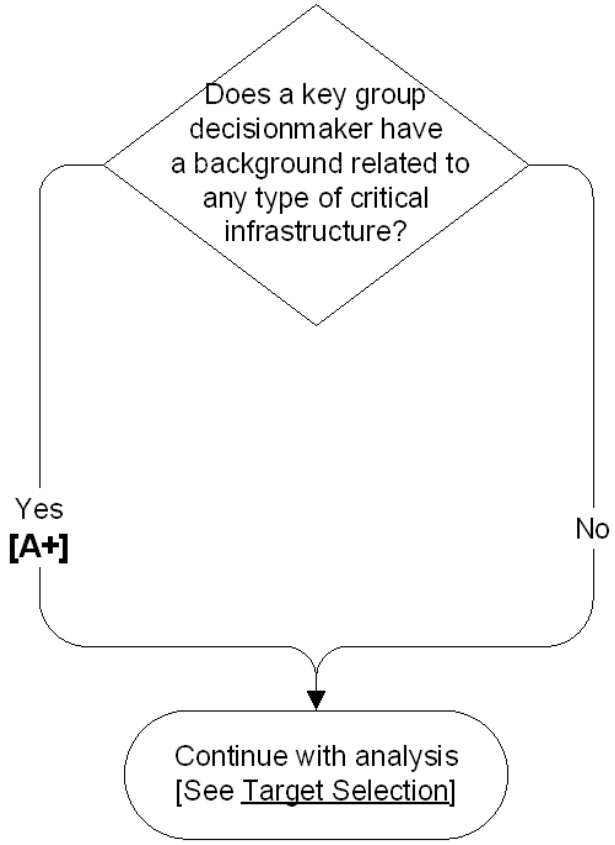
Data Requirements:

- What are the demographic characteristics of key group decision makers, especially in terms of education, vocation, and family background?

Note: The literature neither posited nor implied a direct link between any specific demographic factors and attacks on critical infrastructure. However, the following hypothesis is offered.

Hypothesis: *If a key decision maker has a background or expertise related to any type of critical infrastructure (for instance, if the leader is a civil engineer), this increases the attractiveness of that critical infrastructure as a target.*

If data exists for the above questions, proceed to flowchart. Otherwise, derive inferences from Factor Influences List (following page) and return to the flowchart.



Factor Influence List: Demographics

Ideology affecting Demographics

There is no evidence in the literature surveyed to indicate that ideology impacts demographic factors.

Hypothesis: It is likely that different types of ideologies appeal to different types of people and therefore attract different kinds of recruits. For example, more sophisticated doctrines tend to appeal to better educated people, and vice versa.

Historical Events affecting Demographics

There is no supporting evidence in the literature surveyed to indicate that historical events impact demographic factors.

Hypothesis: certain historical events in which adverse events occurred could have a negative impact on terrorists of certain age groups (e.g. ages 30-60 years), influencing their decision to join a terrorist group and also making them more likely to attack specific types of infrastructure related to or connected with the adverse historical event.

Life-cycle stage affecting Demographics

Hoffmann contends that successor generations of a terrorist group or cause tend to be less idealistic and more ruthless, and may even become expressive.[453] [Evidence Type: 3]

[453] Bruce Hoffman, *Terrorist Targeting: Tactics, Trends, and Potentialities* (Santa Monica: RAND, 1992), p. 5.

Factor Analysis: Resources

Data Requirements:

- What is the general level of the group's financial resources?
- How stable/dependable are current sources of financial resources and what is the cost to the group to obtain them?
- What kinds and amounts of physical resources (weapons, equipment, vehicles, etc.) does the group possess?
- How expansive and sophisticated is the group's logistical infrastructure? Do they have access to safehouses, secure communications, travel documents and so forth? What amount of redundancy is built into the logistics system?

If data exists for the above questions, proceed to the general capabilities framework in target selection. Otherwise, derive inferences to inform the above questions from the Factor Influences List (following page) and then proceed.

Factor Influence List: Resources

Ideology affecting Resources

- There is no evidence in the literature to indicate that ideology impacts resources.
- *Hypothesis: Less ideologically radical groups may in many cases be able to acquire or develop more resources because their goals are likely to appeal to a broader audience and thereby engender the provision of more external assistance.*

Organizational Structure affecting Resources

- Although not specifically mentioned in the literature, it appears to be common sense that larger groups will have access to greater resources – in terms of financial, physical, logistical and human. Bigger groups will require more funding to operate, and they will also have more resources to commit toward increasing their funding and other resources. This could be supported by the arguments advanced by Drake[454] and Jackson.[455]

Demographics and Operational Capabilities affecting Resources

- The logistics network and support systems that an organization sets up for long term as well as short term (attack specific) operations is determined by the demographics of the group as well as organizational structure.[456,457] [Evidence Type: 2,3,4]
- The effectiveness with which the material resources a group possesses in terms of weapons and equipment are used is determined by the operational capability and human resources of a group.[458] [Evidence Type: 1]
- Those groups with members from higher socio-economic strata are more likely to have greater financial and other resources.

External Relations affecting Resources

- State sponsorship of terrorism has infused some terrorist groups with greater resources such as money, sophisticated munitions, intelligence and technical expertise allowing them to contemplate operations larger and more lethal than they would have without state sponsorship. This also removes the constraint of playing to populations for support.[459,460] [Evidence Type: 1]
- State sponsorship of terrorist groups has long been appreciated as a source of advanced weapons technology.[461] [Evidence Type: 1]
- Hoffman identifies state sponsorship with increased capabilities, which could lead to undertaking more ambitious operations.[462] [Evidence Type: 1]
- "Increasingly, terrorist organizations are looking to criminal activity and specifically the drug trade as a source of funding. The FARC in Colombia are but one of many cases in point."[463] [Evidence Type: 3]

Security Environment affecting Resources

- Globalization and a less-regulated environment have allowed terrorists to develop their financial resources.[464] [Evidence Type: 1]

---

[454] Drake, *Terrorists' Target Selection*, p. 73-98

[455] Jackson, "Technology Acquisition by Terrorist Groups," p. 202

[456] Thomas and Casebeer, "Violent Non-State Actors," p. 2.

[457] Drake, *Terrorists' Target Selection,* pp. 54-55.

[458] *Ibid*, pp 88-97.

[459] Brian Jenkins, "Defense Against Terrorism," *Political Science Quarterly*, 101:5 (1986), p.778.

[460] Jackson, "Technology Acquisition by Terrorist Groups," p. 199.

[461] *Ibid*.

[462] Hoffman, *Terrorist Targeting*, p. 16.

[463] U.S. House of Representatives, 106th Congress, Second Session, Subcommittee on National Security, Veterans Affairs, and International Relations of the Committee on Government Reform, July 26, 2000 Hearing, *Combating Terrorism: Assessing Threats, Risk Management and Establishing Priorities* (Washington, DC: Government Printing Office, 2000): http://www.gpo.gov/congress/house, p. 27.

[464] *Ibid*, p. 23.

Critical Infrastructure Characteristics affecting Resources

- CI characteristics can influence a terrorist organization's need to acquire new resources in that the nature of certain types of CI necessitates a certain level of resources for an attack to be successful. Jackson asserts in this regard that the acquisition of new technology by terrorist groups enhances their ability to attack well defended targets.[465] [Evidence Type: 1]

Operational Objectives affecting Resources

- Once terrorists have determined their general operational objectives, they may find that they lack the requisite resources to engage in the type of attack that would give them the effects they seek. This can (but not necessarily will) prompt the group to build up their resources to the levels and types required to perpetrate the desired type of attack. The extra resources can be achieved through, *inter alia*, purchase, theft, indigenous development[466] or transfer from an external supporter.

Target Selection affecting Resources

- *Hypothesis: If a group not only "attacks" CI, but steals from it as well, its resources will grow. Moreover, the more CI attacked, the greater is the non-state actor's knowledge of CI targets.*

Attack Modalities affecting Resources

- As attack modalities become more complex, the resources and operational capability needed to conduct the attack increase in complexity.[467] [Evidence Type: 1,3] *Hypothesis: This can drive the accumulation of greater amounts and more varied kinds of resources.*

Life-Cycle affecting Resources

- *Hypothesis: Although the majority of terrorist groups do not survive longer than a decade, for those groups that persevere for any length of time, it is likely (barring counterterrorist actions to limit this) that the mechanisms for acquiring resources (such as weapons suppliers) will become more regularized, and financial and other resources will accumulate.*

---

[465] Jackson, "Technology Acquisition by Terrorist Groups," p. 195.

[466] "However, for terrorists wishing to carry out more complex operations, training in the use and construction of weapons is extremely useful," Drake, *Terrorists' Target Selection*, p. 81. [Evidence Type: 3]

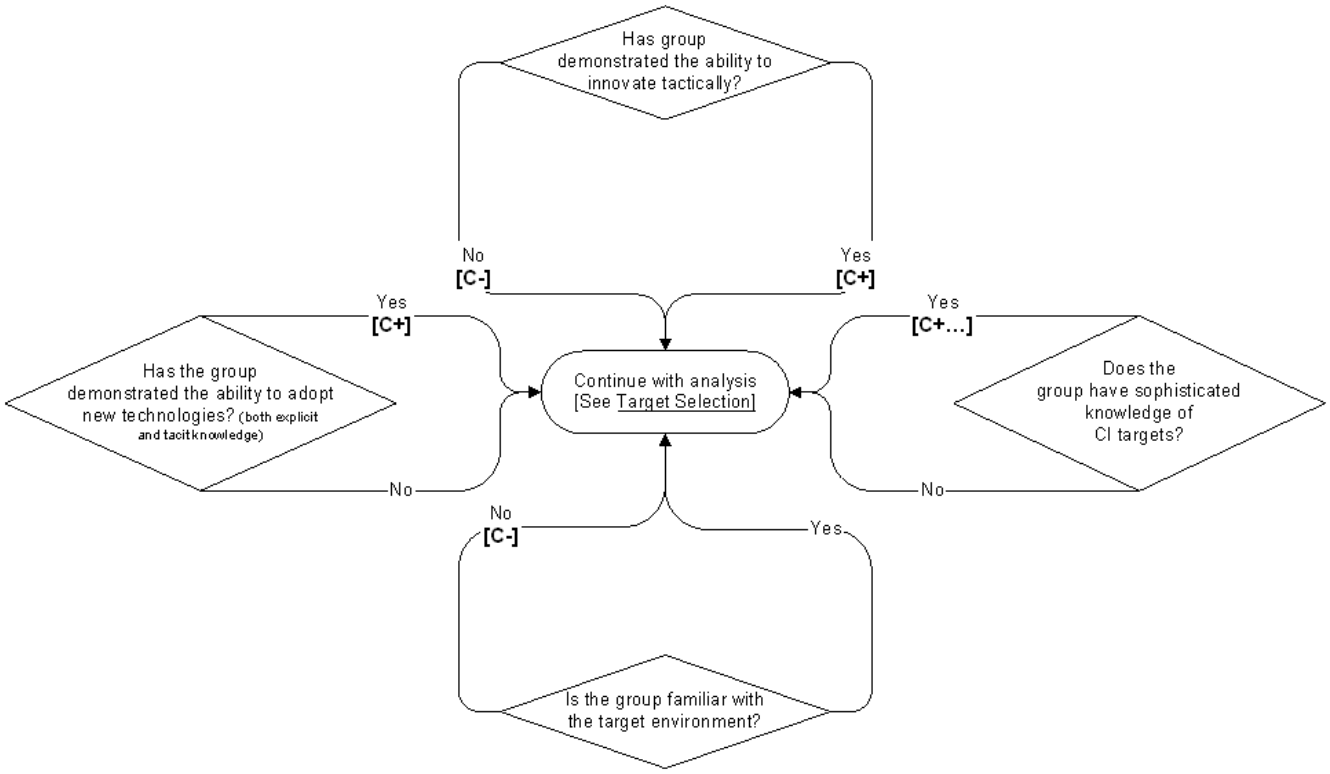
[467] *Ibid*, pp. 54-55, 87-97.

Factor Analysis: Operational Capabilities

Data Requirements:

- What is the group's history of innovation (both tactically and technically)?
- What is the group's general technological level?
- What is the group's knowledge level of various critical infrastructure targets (e.g. through an insider at a nuclear power plant, or someone trained as an roadway engineer)?
- How familiar is the group with the target environment?

If data exists for the above questions, proceed to flowchart. Otherwise, derive inferences from Factor Influences List (following page) and then return to the flowchart. The flowchart must be approached from each side in turn.



Factor Influence List: Operational Capabilities

Ideology affecting Operational Capabilities

- Jackson argues that the "philosophical and ideological views of a group – including both the espoused philosophy of the organization and the 'actual' philosophy revealed by the group's actions – are also critical in determining whether it will seek out new technology." Thus, ideology ostensibly plays a role in a terrorist group's degree of technological innovation. [Evidence Type: 3][468]

Organizational Structure affecting Operational Capabilities

- Jackson uses organizational theory to argue that group structure can influence technological innovation within a terrorist group. Those groups that are cell-based and largely "leaderless" will have more difficulty implementing new technology adoption than will organizations that allow more face-to-face interaction.[469] [Evidence Type: 1,2,4]
- Jackson also states that the size of a group will affect its technical expertise. He notes that the larger an organization, the more likely it is to have members that possess the explicit and tacit knowledge base necessary to efficiently absorb and make use of new technologies.[470] [Evidence Type: 1]
- Drake asserts that a group's size affects its operational capabilities. He notes that a larger organization is more likely to have a richer collection of skills and resources that will enable it to conduct more complex operations.[471] [Evidence Type: 1]
- Drake also suggests that organization size can impact a group's knowledge of CI targets**.** Specifically, larger groups will have the manpower to collect more information about potential targets, enhancing their ability to select good targets which can be effectively attacked.[472] [Evidence Type: 1]

Organizational Dynamics affecting Operational Capabilities

- Jackson points out that "groups led by individuals who are open to new technology" are much more likely to innovate than groups led by individuals hostile to new technology.[473] [Evidence Type: 1]

Demographics affecting Operational Capabilities

- Capabilities, experience, tacit knowledge, and training of members have an effect on the efficiency and effectiveness of the group's operational capability.[474] [Evidence Type: 3]
- *Hypothesis: Socio-economic status, education levels, family background, previous incarceration and substance abuse will all affect the efficiency of the group by influencing the inherent operational capabilities of the members. For instance, the more "worldly" one is the more one might have had experiences with, or an introduction to, a greater variety of targets than one who is rural, poor and uneducated.*
- *Hypothesis: terrorists who have live or been educated in the U.S. may have a clearer understanding of CI locations, access, vulnerability and characteristics; thus, those terrorists could potentially have insider knowledge which could aid and abet in operational planning procedures for future terrorist attacks.*

Resources affecting Operational Capabilities

- Access to resources, especially weaponry, has increased terrorist operational capabilities.[475] [Evidence Type: 3]
- "Off-the-shelf weapons" and improvised explosive devices using commonly available materials have been adapted by terrorists to successfully carry out operations. This has reduced the need to pursue more sophisticated weapons.[476] [Evidence Type: 3] According to Hoffman, "unconventional adaptations and modifications to conventional devices" have given terrorists the ability to carry out effective operations.[477] [Evidence Type: 3]

---

[468] Jackson, "Technology Acquisition by Terrorist Groups," p. 193.

[469] *Ibid*, p. 200.

[470] *Ibid*, p. 202

[471] Drake, *Terrorists' Target Selection*, p. 79-80.

[472] *Ibid*.

[473] Jackson, "Technology Acquisition by Terrorist Groups," p. 193.

[474] Hoffman, "The Modern Terrorist Mindset," pp. 7, 14; Drake, *Terrorists' Target Selection*, pp. 87-88.

[475] Hoffman, *Terrorist Targeting*, pp. 9-11.

[476] *Ibid*, p. 15.

[477] *Ibid*, p. 11.

- Internal and external motivations to innovate increase the technological resources an organization has at its disposal.[478] [Evidence Type: 1] This increases the technical expertise of an organization, which is part of its operational capability.
- Experience, tacit knowledge, and training of members have an effect on the efficiency and effectiveness of the group's operational capability.[479] [Evidence Type: 3]
- State-sponsorship gives terrorist groups access to resources that allows them greater operational capabilities.[480] [Evidence Type: 1]
- The logistics network and support systems that an organization sets up for long term as well as short term (attack specific) operations influence the operational capabilities as well as the resources of the group. This relationship is fundamental in understanding the transference of resources to operational capability.[481] [Evidence Type: 2,3,4]

External Relations affecting Operational Capabilities

- Hoffman[482] [Evidence Type 1] identifies state sponsorship with increased capabilities which could lead to undertaking more ambitious operations. Jenkins[483] [Evidence Type 1] states that state sponsorship of terrorism has infused some terrorist groups with greater resources such as money, sophisticated munitions, intelligence and technical expertise, allowing them to contemplate operations larger and more lethal[484] [Evidence Type 1] than they would have without state sponsorship. This also removes the constraint of playing to populations for support.
- International cooperation between extremist and criminal groups can influence the transfer of expertise and tacit knowledge that leads to an increased operational capability.[485] [Evidence Type 1]

Historical Events affecting Operational Capabilities

- Advances in information technology and the exchange of information have allowed terrorists to propagate successful attack techniques and tools. This medium of accelerated knowledge transfer has reduced the need for training and increased the operational capability of terrorists.[486] [Evidence Type: 1]

Security Environment affecting Operational Capabilities

- Globalization and a less-regulated environment have allowed terrorists to develop their financial resources *and operational capabilities*.[487] [Evidence Type: 1]
- On the other hand, Drake notes that the security environment can restrict a terrorist group's strategy and operational capability and that it is difficult for terrorists to operate in a totalitarian or authoritarian state.[488] [Evidence Type: 1,2]
- Terrorist groups are sometimes motivated to adopt new technology and innovate operational techniques because of changes in the security environment. When the operational capability of a terrorist group has been limited by the security environment, terrorists will adapt to employing unsophisticated low-level attacks on soft targets.[489] [Evidence Type: 1] Terrorists will identify and innovate attack techniques to exploit new vulnerabilities when faced with security environments and countermeasures that nullify existing techniques.[490] [Evidence Type: 3] The resulting competition between terrorists and counterterrorism efforts leads to a "technological treadmill" with each group trying to outdo the other.[491] [Evidence Type: 2,3]

---

[478] Jackson, "Technology Acquisition by Terrorist Groups," pp. 185-187.

[479] Hoffman, "The Modern Terrorist Mindset," pp. 7, 14; Drake, *Terrorists' Target Selection*, pp. 87-88.

[480] Jenkins, "Defense Against Terrorism," p. 778.

[481] Thomas and Casebeer, "Violent Non-State Actors," p. 2; Drake, *Terrorists' Target Selection*, pp. 54-55.

[482] Hoffman, *Terrorist Targeting*, pp. 16-17.

[483] Jenkins, "Defense Against Terrorism," p. 778.

[484] Jackson, "Technology Acquisition by Terrorist Groups," p. 199.

[485] *Ibid*.

[486] Bruce Schneier, *Secrets and Lies: Digital Security in the Networked World* (New York: Wiley Publishing, Inc., 2004), pp. 20-22.

[487] House of Representatives Hearing, *Combating Terrorism*, p. 23.

[488] Drake, *Terrorists' Target Selection*, pp. 121, 123, 178.

[489] Bruce Hoffman, "Al Qaeda, Trends in Terrorism and Future Potentialities: An Assessment. *Studies in Conflict and Terrorism* 26:6 (November-December 2003), p. 437.

[490] Hoffman, "The Modern Terrorist Mindset," p. 16.

[491] Jackson, "Technology Acquisition by Terrorist Groups," p. 184; Hoffman, "The Modern Terrorist Mindset," p. 15.

Life Cycle affecting Operational Capabilities

- *Hypothesis: As a group matures, and gains organizational experience, at least some of its capabilities tend to increase (for example, familiarity with target society and specialized skills).*

Operational Objectives affecting Operational Capabilities

- According to both Bruce Hoffman and Brian Jackson, terrorists display a tendency towards operational conservatism, generally relying more on imitation of their own or others' past successes than innovation of new techniques and technologies.[492] [Evidence Type: 1] They tend to use the same tactics and "off-the-shelf" weapons[493] (albeit often cleverly modified to suit their needs) that they have used for the past half-century. Terrorists usually INNOVATE or pursue a new TECHNOLOGY LEVEL only when they are forced to or feel they will receive unique gains by doing so. The impetus for this change, according to Jackson, can come from the group's operational objectives in the following ways:
    - He argues that groups wanting to dramatically escalate the scale and lethality of their attacks to have a greater punitive or coercive effect may be forced to adopt new weapons and technologies[494] [Evidence Type 1].
    - Groups can feel the need to embrace technologies for ORGANIZATION BUILDING reasons.[495] [Evidence Type: 1]
- *Hypothesis: The type of attack desired (for example, an attack in the heartland of the enemy) may also account for a move to become more familiar with the target society. This could also lead to an increase in a group's networking capabilities if it required the assistance of external actors to accomplish any of the above tasks.*

Attack Modalities affecting Operational Capabilities

- As attack modalities become more complex, the resources and operational capability needed to conduct the attack increase in complexity.[496] [Evidence Type: 1,3]

Perceptual Filter affecting Operational Capabilities

- No direct indications in the literature surveyed that perceptual filter affects operational capabilities, *although cognitive and affect-based biases, if sufficiently powerful, are hypothesized to negatively influence such aspects of operational capabilities as the transfer of tacit knowledge in the technology and skill acquisition process, the extent to which the group can become familiar with a different culture and the ability to successfully network and coordinate with allies.*

---

[492] Hoffman states that, "[T]errorists' traditional arsenal of the bomb and the gun still suffice to exact or win from governments the concessions that terrorists typically seek." Hoffman, *Terrorist Targeting*, p. 16, while Jackson contends that "Organizations, whether they are legitimate or underground, do not innovate for the sake of innovating." Jackson, "Technology Acquisition by Terrorist Groups," p. 189.

[493] Hoffman, *Terrorist Targeting*, p. 15. [Evidence Type: 3]

[494] Jackson, "Technology Acquisition by Terrorist Groups," p. 185.

[495] Increasing the technological or tactical sophistication of an attack may, for instance, be useful to bolster group morale, recruit supporters and compete with rival groups. As Jackson maintains, "…groups that are unable to take advantage of opportunities made available by new technologies risk being displaced from the world stage and surpassed by competitor groups that can." *Ibid*.

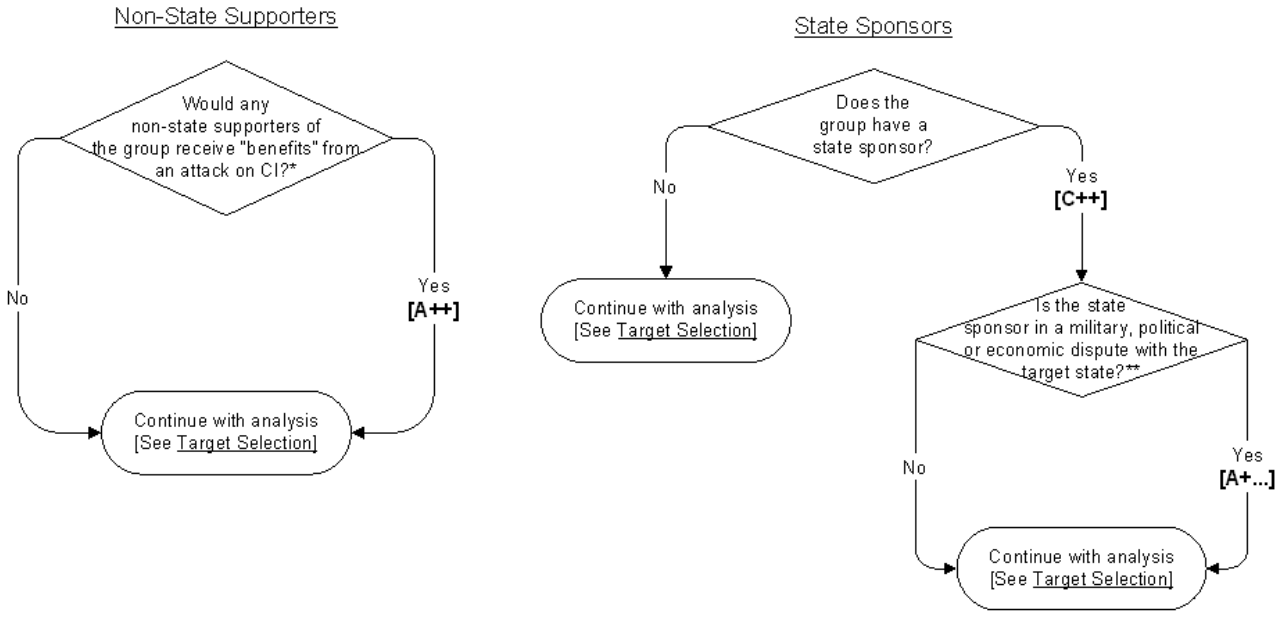
[496] Drake, *Terrorists' Target Selection*, pp. 54-55, 87-97.

Factor Analysis: External Relations

Data Requirements:

- Which external groups or organizations do the terrorist decision makers perceive as allies or potential allies?
- Of these, the support of which external groups or organizations do they seek to gain or maintain?
- Which external groups do the terrorist decision makers perceive as opponents?
- What is the level of publicity terrorists expect from different media groupings?
- How has the media recently portrayed critical infrastructure?

If data exists for the above questions, proceed to the flowchart. Otherwise, derive inferences from Factor Influences List (following the figures on the next page) and then return to the flowchart. Each segment of the flowchart should be visited, where possible.

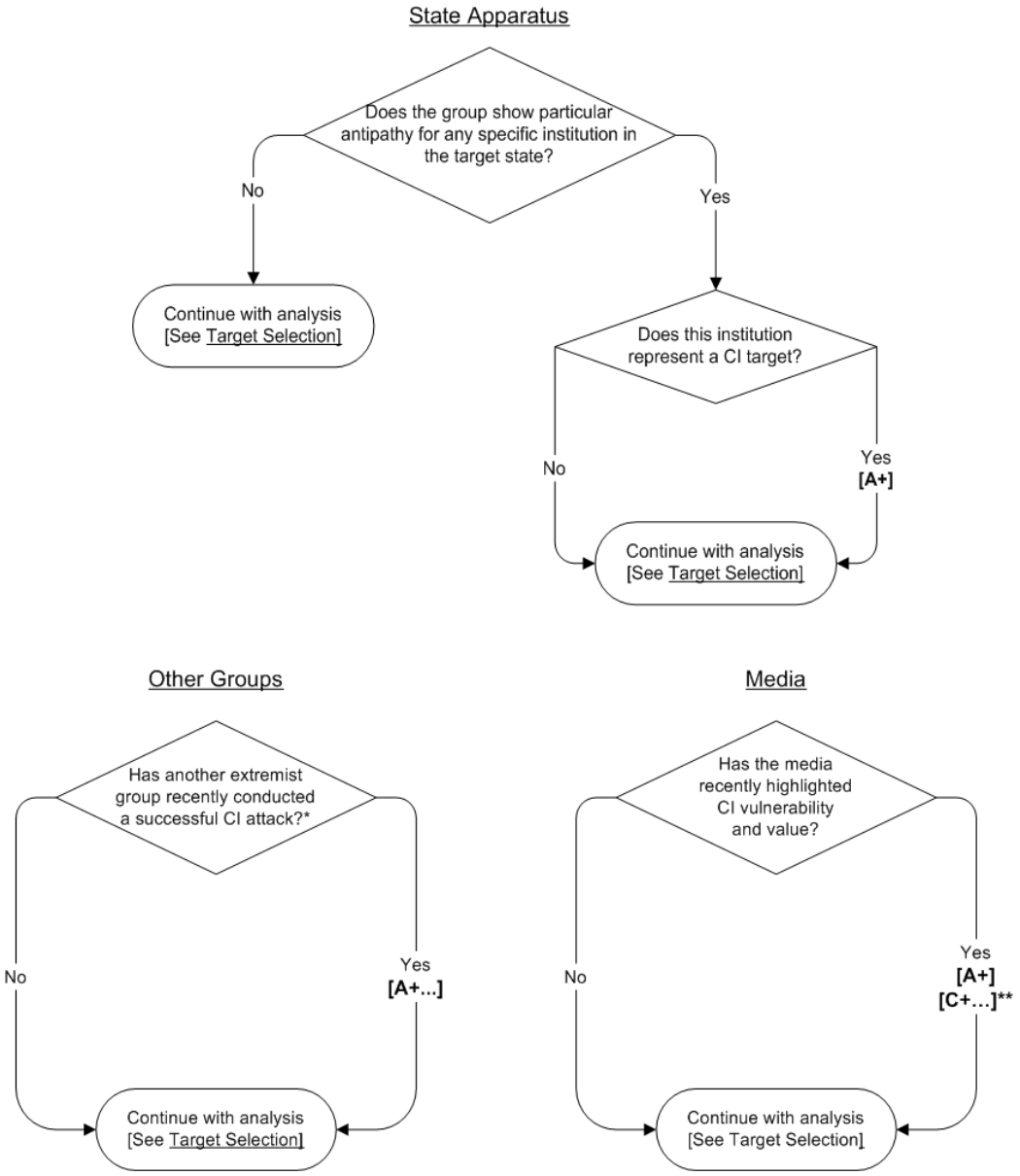


* Group supporters can exert both a direct (by threatening to withdraw active financial and other support) and indirect (by inducing the group to attempt to please its constituency) influence on target selection; if a valued supporter wishes to attack CI targets, the group may comply, all else being equal. Post[497] [Evidence Type: 1] states that when regimes or organizations with known violent aims lend support to terrorist groups there is a greater likelihood of aligning with the goals of the sympathizers or supporters. Cf. also the Chukaku-ha case study in Chapter 3.

** The history of terrorism is littered with examples of state sponsors utilizing terrorist proxies to advance foreign policy goals. In this case, the state sponsor, especially if it perceives strategic gain in a dispute with the target state, may put pressure on the group to inflict tangible economic or other damage on the target state. The effect of this pressure depends on several factors, primarily the degree of dependence on the state sponsor. There is of course always the risk of discovery.

Continue…

[497] Post, Ruby, and Shaw, "The Radical Group in Context," p. 84. [Evidence Type 1]



* Stemming from the imitative nature of terrorist attacks, terrorists may be spurred on by the success of a similar attack by another group. The strength of the increase in attractiveness will depend on several factors, including the degree of success of the previous attack and whether the group under consideration feels it must compete or outdo the perpetrators of the earlier attack. There is "a widely shared expectation that terrorists will return to targets whose importance (and vulnerability) has already been demonstrated" (Baruch Fischhoff, Roxana M. Gonzalez, Deborah A. Small, Jennifer S. Lerner, "Judged Terror Risk and Proximity to the World Trade Center," *Journal of Risk and Uncertainty* 26:2/3 (2003), p. 138).

** By drawing attention to critical infrastructure, the media makes this target more attractive to the group. It may also increase the group's perceived capability by imparting information about the infrastructure that the group perceives as useful in conducting a successful attack. Drake observes that terrorists are less likely to attack targets that are less known among the public. (Drake, *Terrorists' Target Selection*, p. 98).

Factor Influence List: External Relations

Ideology affecting External Relations

- *Hypothesis: Groups espousing ideologies with more widespread appeal and a large constituency will be more likely to acquire a greater number of supporters and sympathizers.*

Resources affecting External Relations:

- Thomas[498] uses systems theory to describe the effect of logistical resources on external relations, "…The support subsystem works at the boundary of the violent non-state actor (VNSA), exchanging energy, monitoring and managing relations with the environment. Five types of environmental transactions are most critical to the VNSA; recruiting, resource acquisition, stakeholder associations, intelligence gathering and product delivery." [Evidence Type: 2, 4]. This implies that poor logistical resources will hamper external relations of all types.

Operational Capabilities affecting External Relations

- *Hypothesis: The lack of sufficient internal operational capabilities may force a group to look for external assistance, making it more likely to want to please its allies*.

Historical Events affecting External Relations

- *Hypothesis: If a terrorist group's ideology addresses events that are historically significant and/or traumatic for a large population, it is likely that the group will have a larger pool of supporters and perceived potential supporters.*

Security Environment affecting External Relations

- *Hypothesis: A more oppressive security environment may a) make it more difficult for terrorists to interact with external parties, such as supporters or the media; and b) make the group more dependent on the assistance of external actors.*

Life Cycle affecting External Relations

- There is no evidence in the literature surveyed to indicate that life cycle affects external relations.
- *Hypothesis: Well-established groups are more likely to have a greater number and variety of external relations than fledgling terrorist groups.*

Target Selection affecting External Relations

- Clearly the targets that are selected will have ramifications with one's constituents and the public at large, but this only occurs after the action has been taken, and so is unlikely to influence external relations DURING the target selection process.

[498] Thomas and Casebeer, "Violent Non-State Actors," p. 2.

Factor Analysis: Critical Infrastructure Characteristics

Data Requirements:

- What is the level of protection decision makers perceive CI targets in general (relative to other targets) or particular CI targets of interest, to have?
- What does the group perceive the functionality of the target to be and the consequences they expect from a successful attack against the CI target?*
- What is the level of publicity they expect to receive by attacking that particular target?**

This is a vital element of the analysis. If data exists for the above questions, proceed to further factor analyses. Otherwise, derive inferences from Factor Influences List (following page) and then move on.

*The extent of the political, economic, and military costs suffered by a target society or group due to the loss or disruption of a target plays an important role in the terrorist selection of target. Such damage, termed impact loss by Renfroe and Smith, constitutes an important factor in the selection of targets. Renfroe and Smith posit that a target that has a high impact loss and a high degree of vulnerability will be an ideal choice for terrorists.[499] We argue that this applies more accurately to the impact loss and vulnerability associated with a target as perceived by the terrorist group, which in most, but not all, cases will reflect the true impact loss and vulnerability. Targets that terrorists perceive to have a cascading or 'knock-on' effect that spreads far beyond the site of attack are therefore presumed to be especially attractive to a terrorist group seeking disruption on a massive scale.

** Renfroe and Smith also maintain that a target with a high symbolic value or utility increases its attractiveness to a terrorist.[500]

---

[499] Nancy A Renfroe and Joseph L. Smith, "Threat/Vulnerability Assessments and Risk Analysis," *Whole Building Design Guide*. Accessed on 03/11/2004 at http://www/wbdg/org/design/res-print.php?rp=27, pp. 2-3.

[500] *Ibid*.

Factor Influence List: Critical Infrastructure Characteristics

Since the characteristics of critical infrastructure are exogenous factors, rarely dependent on anything the group does DURING the decision process, there are no direct group factors that can influence target selection. However, the general security environment can affect the critical infrastructure directly, and of course, several factors influence the terrorist group's perception of these CI characteristics. These latter factors are dealt with during the 'target selection' phase of the analysis.

Security Environment affecting Critical Infrastructure (CI) Characteristics

- It is commonsense that the general security environment is linked to the level of target protection. As general alert levels and security measures increase, it can be assumed that the protection around many targets will increase. A heightened security alert status will in most circumstances lead to better protection measures around CI facilities that are not as highly guarded under less threatening circumstances. However, this will not necessarily be the case (since the actual implementation of specific measures is dependent on several other variables such as the defender's resource constraints, political considerations, and competence).

Factor Analysis: General Planning Characteristics

Data Requirements:

- Do group decision makers have a set timetable for action?
- How tolerant are decision makers about risk (in terms of operational success, group survivability and the welfare of group members)?

This element of the analysis has no direct effect on target selection, but may influence other factors. If data exists for the above questions, nothing need be done. If not, inferences from the Factor Influences List (following) can be derived in order to inform other areas of the framework.

Factor Influence List: General Planning Characteristics

Ideology affecting General Planning Characteristics

- Nothing in the literature surveyed indicates a relation between the ideology of a terrorist group and the general planning characteristics for an attack.
- *Hypothesis: Ideology can affect both a terrorist group's time horizon and risk tolerance. Certain ideologies, for instance, that of an apocalyptic cult, may set a timetable for action that gives decision-makers a limited time horizon. Other ideologies, especially in terms of the value they place on group member's lives and the notion of 'sacrifice', may make a group more or less tolerant of risk.*

Organizational Dynamics affecting General Planning Characteristics

- Nothing in the literature surveyed indicates a relation between the organizational dynamics of a terrorist group and the general planning characteristics for an attack.
- *Hypothesis: Intra-group dynamics can impose perceived deadlines, for instance a challenge to the leadership may make the existing leader perceive that an operation is needed more urgently.*

Operational Capabilities affecting General Planning Characteristics

- Nothing in the literature surveyed indicates a relation between the operational capabilities of a terrorist group and the general planning characteristics for an attack. *However, the operational capabilities possessed by the group are likely an important factor in the group's assessment of time requirements and the risks associated with a particular attack.*

CI Characteristics affecting General Planning Characteristics

- Nothing in the literature surveyed indicates a relation between the characteristics of potential CI targets and the general planning characteristics for an attack.
- *It can be argued, however, that terrorists consider the characteristics of the target in performing risk assessment and evaluating the time requirements for an attack. For instance, a facility that is in the process of increasing its level of protection may prompt terrorists to consider attacking the facility before the increased security is in place.*

Historical Events affecting General Planning Characteristics

- Post describes triggering events as events which lead a group to believe that the only course of action involves violence. Some triggering events may increase the risk of terrorism. [Evidence Type: 1][501]
- Pynchon adroitly describes the effects of historical events on the perceived time horizon of decision makers: "Situational changes may increase a group's sense of urgency. A heightened sense of urgency may increase the propensity for violence…"[502]
- *Hypothesis: Terrorist attacks often occur (as a retaliatory or punitive measure) on the anniversary of an event which the group perceives as an adverse historical event. This can impose time constraints on decisions.*

Security Environment affecting General Planning Characteristics

- *Hypothesis: A more oppressive security environment increases the group's perception of threat and therefore may narrow their perceived window for planning and action.*

Perceptual Filter affecting General Planning Characteristics

- The perceptual filter is closely linked to risk tolerance and decision maker time horizon, since these factors will be affected by any perceptual distortions that may be operating.[503]

---

[501] Post, Ruby, and Shaw, "The Radical Group in Context," p. 98.

[502] Marisa Reddy Pynchon and Randy Borum, "Assessing Threats of Targeted Group Violence: Contributions from Social Psychology," *Behavioral Sciences and the Law* 17, (1999), p. 348. [Evidence Type: 1]

[503] See the discussion of the Perceptual Filter in Chapter 2 for details.

Operational Objectives affecting General Planning Characteristics

- The specific operational objectives set by the group during the attack planning process can have an obvious and direct effect on the decision maker's time horizon, in that certain of these objectives may be time-dependent. An illustrative example is the case where a decision maker wants to act to increase recruitment relative to a rival group – if he delays too long, the competitor may induct the best personnel from among the pool of available recruits and the objective of increasing recruitment may remain unfulfilled no matter how successful the attack ultimately turns out to be.
- Joshua Sinai describes the different incubation periods associated with different types of attack and asserts that high-impact conventional and CBRN attacks generally require longer incubation periods than low-impact conventional attacks.[504] [Evidence Type: 3]
- Drake mentions that in certain cases, once a group decides on a general category of targets, they will attack as soon as a specific target within that group presents itself.[505] [Evidence Type: 1]

[504] Sinai cites the following examples: "the 1993 World Trade Center bombing was preceded by five months of preparations; the Aum Shinrikyo attack in 1995 was preceded by attempts that lasted for about a year; the 1995 Oklahoma City bombing plot began six months earlier; the Cole attack was reportedly planned for eight or ten months and the 9/11 attacks were preceded by a two-year incubation period. Conventional, low-impact attacks are prepared quickly, generally in three to five days or less, so there is a much shorter window of opportunity to preempt such attacks." [Sinai, "Analytical Model of Terrorism Forecasting," #75 p. 3]

[505] Drake, *Terrorists' Target Selection*, p. 56.

Factor Analysis: Perceptual Filter

Data Requirements:

- Do any key group decision makers exhibit clear symptoms of psychopathologies that could lead to perceptual impairment?
- Is there evidence that group decision makers habitually exhibit particular cognitive or affect-based biases? If so, which biases dominate and how do these tend to manifest?*

* See discussion of the perceptual filter in Chapter 2 for details of possible biases.

This element of the analysis has no direct effect on target selection, but certainly influences other factors, the extent dependent on the strength of the perceptual impairment. If data exists for the above questions, proceed to the Target Selection section. If not, derive inferences from the Factor Influences List (below) and then proceed to Target Selection.

Factor Influence List: Perceptual Filter

Ideology affecting Perceptual Filter

- *Hypothesis: At least some portion of the various 'frames' through which information is processed is determined by the ideology, particularly the worldview, of the group. For example, a group whose ideology is religiously based may define another religious group as irretrievably corrupt enemies of god and therefore any actions by this enemy, however benign or logical, will be perceived as stemming from, and confirming, his evil.*

Historical Events affecting Perceptual Filter

- *Hypothesis: Similarly to the mechanisms by which historical events can impact a group's ideology, they can also influence the way in which group decision makers interpret information, particularly that flowing from the outside world. Thus traumatic events in the lives of decision makers can bias their perceptions of the information they receive.*

Demographics affecting Perceptual Filter

- *Hypothesis: A correlation can be made between psychological health and perceptions. Psychologically unstable individuals within a terrorist group will perceive things differently than normal, stable individuals.*

Security Environment affecting Perceptual Filter

- An increasingly oppressive security environment can place group members under prohibitive levels of stress and can exacerbate existing perceptual impediments.

General Planning Characteristics affecting Perceptual Filter

- Pynchon describes how the perceived time horizon of decision makers can affect the perceptual filters through which information passes to decision makers: "Situational changes may increase a group's sense of urgency. A heightened sense of urgency may increase the propensity for violence by 1) increasing the likelihood of irrational reaction to a triggering event, [and] 2) increasing the likelihood of "flawed decision-making" re targeted violence..."[506] [Evidence Type: 1]

Life Cycle affecting Perceptual Filter

- The perceptual filter of the group will undoubtedly change during the group's lifetime, as decision makers change and external and internal events shape the cognitive outlook of the group. It is extremely difficult to predict the direction of these changes, whether, as Hoffmann implies[507], affect-based distortions become more pronounced, or, conversely, that new leadership structures emerge with fewer information processing biases.

Demographics affecting Perceptual Filter

- There is no supporting evidence in the literature to indicate that demographic factors impact perceptual filters.
- *Hypothesis: a correlation can be made between age and perceptions, as different age groups will have different perceptions; which may ultimately affect their operational planning methods.*
- *Hypothesis: Psychologically ill decision makers may experience cognitive impairment of various types.*

---

[506] Pynchon and Borum, "Assessing Threats of Targeted Group Violence," p. 348. [Evidence Type: 1]

[507] "Not only are successor generations smarter than their predecessors, but they also tend to be more ruthless and less idealistic. For some, in fact, violence becomes almost an end in itself—a cathartic release, a self-satisfying blow struck against the hated "system"—rather than being regarded as the deliberate means to a specific political end embraced by previous generations." Hoffman, *Terrorist Targeting*, p. 5. [Evidence Type: 3]

Step 4: Determination of Intent

Operational Objectives Analysis

This element is integral to the analysis and must be completed. It is essential to have read and understood the definition of Operational Objectives in Chapter 2. This part of the analysis serves primarily as a limiting exercise to verify that critical infrastructure is not excluded from the target set. It may also in certain circumstances reveal a particular orientation that points towards critical infrastructure targets.

Table 5.1: Operational Objective Categories

Objective Category *Explanation*	**Punitive** *[desired effect: hurt enemy]*		**Coercive** *[desired effect: get enemy to alter his behavior]*		**Organization-Building** *[desired effect: to assist terrorists' own organization]*		**Enemy Capability-Diminishing** *[to decrease the ability of the enemy to oppose the terrorist group (non-coercive)]*	
Specific Outcome Objectives	1 a) Revenge (retribution for long-standing perceived injury)		Weaken opponent's will to oppose group goals (through fear)	P	Acquire physical resources	I	Eliminate opponent's military / security forces	I
	1 b) Retaliation (retribution for recent perceived injury)		Draw attention to group's cause	P	Boost internal morale*	P	Disrupt opponent's military / security forces	I
	1 c) Eliminate Enemy Population	I	Show opponent to be vulnerable / impotent	P	Increase recruitment*	P	Distract opponent's military / security forces	I
			Disorient opponent	P	Increase external support*	P		
			Provoke government backlash		Influence intragroup power relations* (reinforce status quo or bolster challenge)	P		
			False flag operation	P				
Attack Types	Harm population (low-high)		Harm population (low-high)		Harm population (low-high)		Harm military / security forces (low-high)	
	Destroy infrastructure (high only)		Actions that threaten harm (low-high)		Actions that threaten harm (low-high)		Destroy military / security infrastructure (low-high)	
	Disrupt infrastructure (high only)		Destroy infrastructure (low-high; high likely)		Destroy infrastructure (low-high)		Disrupt military / security infrastructure (low-high)	
			Disrupt infrastructure (low-high; high likely)		Disrupt infrastructure (low-high)			

* In relation to other organizations, potential organizations or non-participation.

Notes on Table 5.1

a) Attack Types: For purposes of this project, attack types are divided into four categories: those attacks directed towards harming people; those that threaten to harm people (such as hostage-takings); those intended to destroy infrastructure (e.g. to destroy a power plant utterly); and those intended to disrupt infrastructure (for a limited amount of time). Note that infrastructure attacks in this case are not necessarily against critical infrastructure, but against any types of infrastructure. The attack types listed in each column are those that can be used to fulfill the objectives in that column.
b) The low-high annotation in the attack type portion of the table refers to the scale of attack/impact that would be required for each attack type in order to fulfill that objective type. So, for example, looking under the heading of "Organization Building" the scale of the attack type to "harm population" can run from high to low, depending on circumstances, while, under the "Punitive" category, an infrastructure attack would need to have a high impact in order to fulfill the an objective like revenge.
c) *Publicity* can be regarded as a corollary operational objective category – it is not useful in and of itself but may be a necessary adjunct to other purposes. Rationales for attack where publicity is likely to be most important are indicated by a 'P'.
d) Categories marked with an 'I' indicate that they require an *Instrumental* target only (i.e. a symbolic element is not needed). All other categories generally require a symbolic element or some other means to gain publicity such as attack novelty or scale[508]. Publicity is important for all symbolic attacks.

Many of the factors related to the motivation to attack a critical infrastructure target have already been addressed earlier in the analysis. Those that have not been are dealt with below as aspects of "Attractiveness" and "Target Set."

Attractiveness

One important aspect to consider in terms of the attractiveness of critical infrastructure as a target set is the desired impact of the attack; if there is any evidence indicating the scale or impact that the particular group intends, this can affect the attractiveness of a CI target.

Is there evidence to suggest that the group will specifically seek to perpetrate a high-impact attack?

> *If the answer is NO, and a low-impact attack is sufficient to fulfill group goals, then an attack directed towards crippling critical infrastructure in a developed country like the United States is less necessary and the attractiveness of a high-impact critical infrastructure target decreases,*[509] *i.e.*, [A-].

Target Set

We begin the target set limitation exercise at the operational objectives stage, instead of beginning by looking at ideology explicitly, due to the observation made by Drake[510] that on occasion terrorist groups have been known to step outside the boundaries of their ideological constraints if the strategic benefits of an attack outweigh the boundaries set by ideology. While this may happen only rarely, one cannot therefore set a rigid boundary condition at the ideology stage; the framework however takes into account the strong influence of ideology

[508] Of course, any category CAN have a desired symbolic effect, even if it is not necessary.
[509] Of course, a small-scale attack against critical infrastructure targets or a large-scale attack against ordinary (non-critical) infrastructure targets is still feasible, but the time, risk, and resources associated with an attack designed to have a high-impact on critical infrastructure can be expected to make such an attack less appealing.
[510] Drake, *Terrorists' Target Selection,* p. 181.

implicitly through the factor influences on operational objectives and explicitly through the attractiveness indicator, where ideological factors have a significant (although not determinative) influence.

The following procedure builds on previous analysis, with the express purpose of verifying that CI attacks are not excluded or prescribed.

1. Answer the following questions using your answers (both inferred or known) to the questions in the Master Data Requirements List, or by further inference from the Factor Influence List (see page after next):

General:

a) Is there any evidence of a specific dominant outcome objective[511][found in the second section of Table 5.1]?
If so, note this outcome objective.
b) If there is insufficient evidence of a specific desired outcome, is there any evidence that the group is currently seeking a specific type of objective (or set of objective types)? [i.e. is the group primarily oriented towards a punitive, coercive, organization-building, or enemy capability-diminishing type of attack?]
If so, note the objective type or set of objective types.
Hypothesis: all else being equal, attacks with primarily punitive objectives, where the degree of enmity is great, are generally less likely to be against critical infrastructure alone (i.e. without substantial casualties involved).

Casualties:

Are high casualty levels desired?
If so, then a critical infrastructure attack is still possible, but any critical infrastructure target must include large numbers of potential human victims.
Are high casualty levels tolerated[512]? [Remember to also take into account the tolerance of group supporters and its perceived constituency, which most groups will pay attention to.]
If the answer is NO, then the target set is substantially limited.

Mitigating Factors:

Is the group dependent upon or does it perceive benefits from certain types of critical infrastructure in its target area[513]?
If so, then those particular types of critical infrastructure will likely be excluded from the target set.

Impact Type:

Is there any evidence that the group specifically wants to cause economic damage to its enemies?
If so, the feasible target set is further limited, and the restricted set does include critical infrastructure targets.

---

[511] This assumes, since the analyst has proceeded past Step 1 of the framework, that the analyst does not know that the group specifically intends to attack critical infrastructure.
[512] Although this question has already been considered previously, the earlier context was an exclusion of casualties due to ideology; there may be several non-ideological reasons, including not wanting to alienate supporters, why groups may find high casualties intolerable.
[513] For instance, if the group is highly dependent for its communications on the Internet, and there are no specific reasons for disrupting the Internet and other targets are plentiful, the group would tend to exclude the Internet from its target considerations.

Publicity:

What scale of publicity does the group need or desire (e.g., local; national; global)? [Table 5.1 indicates where publicity is most important.]
If the group needs or seeks a large amount of publicity, are there critical infrastructure targets that group decision makers could perceive as generating an especially high degree of publicity?

If YES, this means that critical infrastructure is in the restricted target set. An attack truly intended to cripple critical infrastructure is automatically a terrorist 'spectacular'.

2. Bearing in mind the progressive restriction of target space process (see Figure 5.2), use Table 5.1 and your answers to the above questions to limit the range of operational objectives and thereby the target set. Even if infrastructure (as shown in the table) remains within the target set, one still needs to take into account the desired SCALE of the attack, since critical infrastructure attacks are by definition high-impact attacks. This process, together with the information collected and analyzed during the individual factor analyses should verify whether or not critical infrastructure targets remain in the target set and, in some cases, inform the analyst whether or not critical infrastructure is the only element left in the likely target set.

   Examples:

   a) A group wanting to punitively eliminate the population of its enemy is unlikely to target critical infrastructure above a mass-casualty target such as bombing a music concert[514].
   b) A group with the desire to show their opponent as impotent and vulnerable, seeking a high-impact attack, but whose supporters are intolerant of casualties, is left with few target options in the restricted target space besides a critical infrastructure target.

[514] Attacks on certain critical infrastructure targets could result in mass casualties (for instance chemical plants), although the motivation here would not be an attack on the infrastructure itself (to disable or disrupt its functioning) as much as using the plant as a means of causing mass casualties.

Factor Influence List: Operational Objectives

Ideology affecting Operational Objectives

- Most commentators would agree that ideology is a major (but not necessarily a determinative) causative factor in the effects terrorists seek to achieve through their attacks. Drake posits that ideology influences an attack in a direct manner in that a group's specific worldview can prescribe specific operational objectives. [Evidence Type: 3][515] *Inference: Likewise, that worldview can proscribe certain objectives.*
- Drake also believes that a group's ideology limits the set of legitimate targets terrorists are willing to consider, and it is this limited set that terrorists consider attacking in an effort to achieve their operational objectives.[516] [Evidence Type: 1] One example of this has to do with the terrorists' attitudes towards causing human casualties. Parachini[517] implies that certain worldviews lead to a specific desire to cause as many casualties as possible. [Evidence Type: 1]
- Ideology does not have a determinative influence on operational objectives - in certain cases those objectives may stray out of the bounds set by the ideology (e.g., as per Drake's formulation, when the perceived strategic benefits of eliciting a significant reaction from the psychological target outweigh certain ideological prohibitions[518]). [Evidence Type: 3]
- The influence of ideology on operational objectives also depends on whether the terrorist group in question views violence as a means to an end or an end in itself [Evidence Type: 3][519] *Hypothesis: When violence is regarded as a means to an end, the operational objectives of an attack are more likely to be constrained by the group's overall ideology. However, in cases where a group's ideology actually views death and destruction as a goal in and of itself (e.g. an apocalyptic cult), ideology is less likely to impose limits on operational objectives and may in fact expand the target options available to terrorists.*
- *Hypothesis: ideology can affect admissible casualty levels in the following ways:*
    - *if low casualty levels are desired or tolerated, this will limit the range of targets*
    - *if high-casualty levels are tolerated, any target will be suitable*
    - *if high-casualty levels are desired, that too will limit the range of prospective targets*

Organizational Dynamics can affect Operational Objectives

- Internal group pressures can affect the decision makers' ability to articulate their operational objectives rationally.[520] [Evidence Type: 1].
- Operational objectives may in general be bounded by ideological concerns, but in the short term – during a single attack process – these objectives will be interpreted and prioritized by key decision makers; therefore, if the leadership of a group changes, the new leaders may not have the same strategic outlook[521] [Evidence Type: 3]. Post argues that LEADERSHIP STYLE – in particular, psychotic, narcissistic and paranoid leadership personalities – can affect the likelihood of groups to tend toward violence, in that the above-mentioned personality types may be prone to seeking increased levels of violence (including casualties).[522] [Evidence Type: 2]. *Hypothesis: PSYCHOLOGICAL HEALTH – clinically unstable decision makers (such as sociopathic personalities) may be less likely to be bound by ideological and other constraints when looking at operational objectives; they may, in many cases, be more likely to act punitively in addition to fulfilling other goal types.*
- Severe FACTIONALIZATION or imminent splitting within a group can lead to more extreme operational objectives (and their subsequent retroactive endorsement), as per Drake, who states that actions by "more

---

[515] Drake, *Terrorists' Target Selection*, p. 36.

[516] *Ibid*, pp.178, 181. Drake posits that "…it might be the case that the terrorists concerned could gain strategic benefits by attacking a target which is not seen as being a legitimate target. For the terrorists themselves this may or may not represent a dilemma. Some terrorists may decide that attacks cannot be made against targets which do not bear some form of guilt in terms of the ideology of the terrorist group concerned, whilst others may feel that the very fact that attacking a particular target fulfills a strategic objective makes it a legitimate target." p. 178.

[517] Parachini, "Comparing Motives and Outcomes of Mass Casualty Terrorism," p. 403.

[518] Drake, *Terrorists' Target Selection*, p. 181.

[519] McCormick, "Terrorist Decision Making," p. 480.

[520] Drake, *Terrorists' Target Selection*, p. 35.

[521] *Ibid*, p. 37.

[522] Post, Ruby, and Shaw, "The Radical Group in Context," p. 85.

violent or impetuous members of a group, can force the leadership to endorse such actions retrospectively for fear of losing the group's internal cohesion or even splitting the organization."[523] [Evidence Type: 1].

- *Hypothesis: in groups where FACTIONALIZATION occurs or is imminent, a 'challenger' faction may push for greater scale or more extreme desired effects than otherwise as part of a power play. Also, a 'status quo' faction may feel the need to increase the scale or effects of an attack in order to bolster their position within the group and undermine challengers.*

Resources affecting Operational Objectives

- According to his definition of strategy[524], Drake implies that terrorists take into account their available resources when deciding on a course of action. As previously mentioned, Drake's construction differs somewhat from our conception of operational objectives. While it can be assumed that terrorists will keep their present resource levels in mind throughout the attack planning process, it is usually only at the stage of preliminary target selection, when they already have an idea of what they want to achieve by an attack, that resources (through the consideration of group capability) are explicitly accounted for. Operational objectives are therefore likely to have a much stronger influence on resource levels than the converse relationship.

Operational Capabilities affecting Operational Objectives

- Similar to the discussion regarding resources, while it can be assumed that existing operational capabilities will be borne in mind throughout the attack planning process, it is usually only at the stage of preliminary target selection, when terrorist decision makers already have an idea of what they want to achieve by an attack, that they explicitly consider their operational capabilities and resources (through the determination of group capability). Operational objectives will thus in the vast majority of cases exert more of an influence on operational capabilities than vice versa.
- *Hypothesis: a group possessing a technology, tactic, skill or weapon it feels is unique (such as expertise in skydiving), may become biased toward using this capability when deciding on operational objectives.*

External Relations affecting Operational Objectives

- One of the first things to keep in mind is Jenkins'[525] argument that the effect of violence on people watching the violent act (such as the general public or the government) is perhaps as important and maybe even more important than the physical damage inflicted. [Evidence Type 1]
- Hoffman[526] indicates that although in many cases less spectacular attacks are considered by terrorists to be legitimate and acceptable as a means to influence the general public**,** the public can experience a level of desensitization where "typical" targets no longer garner the desired reaction and this drives the terrorists to more violent and dramatic acts to regain attention. [Evidence Type: 1] He states that "…for many other terrorists…equation of publicity and attention with success and self-gratification has the effect of locking them into an unrelenting upward spiral of violence in order to retain the media and public's attention…The effect is that terrorists today feel driven to undertake ever more dramatic and destructively lethal deeds in order to achieve the same effect that a less ambitious or bloody action may have had in the past."[527]
- Hoffman further contends[528] in the case of ethno-nationalist/separatist terrorist organizations, that the more successful groups 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 modulated so as not to provoke massive governmental crackdown and reaction. [Evidence Type: 1]
- Sinai argues that external relations – in particular, links with foreign groups and state sponsors – will affect an organizations willingness to attack.[529] [Note: He does not specifically say how, but implies that the organization will act in a manner consistent with the norms of its constituency groups.] Jackson presents a variation on this sentiment by arguing that some groups will make decisions to attack based on the need to achieve recognition and "respect" from external groups.[530] [Evidence Type: 2]

---

[523] Drake, *Terrorists' Target Selection*, p. 171

[524] "Strategy is taken to be the plan by which a terrorist group seeks to deploy and use its resources with the aim of achieving its political objectives," *Ibid*, p. 35. [Evidence Type: 2]

[525] Jenkins, "Defense Against Terrorism," p. 776.

[526] Hoffman, "The Modern Terrorist Mindset," p. 13

[527] *Ibid*.

[528] *Ibid*, p. 4.

[529] Sinai, "Analytical Model of Terrorism Forecasting," p. 2.

[530] Jackson, "Technology Acquisition by Terrorist Groups," p. 185.

Historical Events affecting Operational Objectives

- The Influence of Previous Attacks:
  - In general, past behavior has been shown to be a good (but by no means foolproof) guide to 'types' of future behavior – as seen in the threat assessment of individual suspects (see Corcoran and Cawood).[531] In assessing the likelihood that an individual may be involved in violent activities, Fein, Voseekuil, & Holden explain that it is important to know if the subject has expressed interest in particular targets, has attempted to harm self or others, has practiced with weapons, and has approached potential targets.[532] Experience from the study of individual violence probably carries over to some degree to the context of a terrorist group. [Evidence Type: 1]
  - If previous attacks (targets, tactics, weapons etc.) are viewed by a group as successful, and they perceive such attacks will be successful in the future, this may encourage some groups to emulate these attacks; however, groups (especially those seeking to put themselves on the map or to outdo competitors) also may want to 'do one better' and escalate SCALE if not target type. A combination of the ideas of Nacos,[533] Woo[534] and Hoffmann[535] supports this.
  - The notion of adaptive learning: Al-Qaeda seems to follow this, as per Woo: "Al Qaeda is eager to learn from past terrorist experience – the successes and failures of attacks perpetrated by its own network, and by other terrorists around the world."[536]
  - People tend to overestimate past events in terms of success – this is a form of attribution bias and is described in Taleb.[537]
- Relative Global Discrepancies:
  - A report of the Subcommittee on National Security, Veterans' Affairs, and International Relations argues that the United States may continue to become a more desirable target due to continued economic, political, and military growth.[538] [Evidence Type: 1]

---

[531] Michael Corcoran and James S. Cawood. *Violence Assessment and Intervention: The Practitioner's Handbook* (Boca Raton: CRC Press, 2003).

[532] Robert A. Fein, Ph.D; Bryan Vossekuil; and Gwen A. Holden, "Threat Assessment: An Approach to Prevent Targeted Violence," *NIJ Research In Action* (September 1995), pp. 3-4.

[533] "The idea of the calculus behind the 9-11 attacks serving as a model for future terrorism is not far fetched, if the operation was and continues to be deemed successful by group and individuals already involved in or pondering political violence." Brigitte L. Nacos, "The Terrorist Calculus behind 9-11: A Model for Future Terrorism;" *Studies in Conflict and Terrorism* 26 (2003), p. 2. [Evidence Type: 1]

[534] "The more often an attack mode has been used, the more likely it is to be re-used in another terrorist operation." Gordon Woo, "The evolution of Terrorism Risk Modeling," *The Journal of Reinsurance* (April 22, 2003) p. 6. [Evidence Type: 1]

[535] "[T]errorists consciously learn from one another" Hoffman, "The Modern Terrorist Mindset," p. 7. [Evidence Type: 3]

[536] "'Avoid strength, and attack weakness'…asymmetric warfare…For Al Qaeda, this may be expressed in the succinct language of physical science as: *follow the path of least resistance*… adaptive learning. Al Qaeda is eager to learn from past terrorist experience – the successes and failures of attacks perpetrated by its own network, and by other terrorists around the world. Al Qaeda would tend to 'copycat' methods which either have proven to be successful, or are perceived to have the potential to be successful. If an attack mode has demonstrated effectiveness, or has the promise of being effective, it is likely to be an attack option." Gordon Woo, "Understanding Terrorism Risk," Risk Management Solutions, http:// www. rms.com/Publications/UnderstandTerRisk_Woo_RiskReport04.pdf, p. 7. [Evidence Type: 1]

[537] "Agents overestimate their skills owing to attribution bias…Individuals ascribe their past failings to random events, but their successes to their skills. The consequence is that their projection of the space of eventualities will be rosy and they will underestimate the incidence of possible setbacks…People are unaware of their own track record and do not learn that their past projections were too optimistic and correct for it." Nassim Nicholas Taleb, "The Black Swan: Why Don't We Lean that We Don't Learn?" draft of paper prepared for Highland Forum #23, January 2004, pp. 25-27. [Evidence Type: 1]

[538] The House of Representatives Hearing, *Combating Terrorism*, p. 23.

- Trigger Events:
    - Post describes trigger events as events that lead a group to believe that the only course of action involves violence. An example of a triggering event is when group members or leaders are harmed by a regime or other opponent.[539] [Evidence Type:0 2]
    - *Hypothesis: the nature of the trigger event can lead to specific operational objectives, for example, the desire to regain legitimacy by causing casualties, or an increase in the desired scale of an attack.*

Security Environment affecting Operational Objectives

- One opinion holds that when the operational capability of a terrorist group has been limited by the security environment, terrorists will adapt to employing unsophisticated low-level attacks on soft targets.[540] [Evidence Type: 1]
- On the other hand, Pynchon suggests that the security environment – specifically, the levels of vulnerability and threat a group feels – may be directly correlated to a terrorist group's willingness to coalesce around more violent acts.[541] [Evidence Type: 1]
- Drake implies that external pressures on the group stemming from increased pressure from the security forces can influence the group's choice of operational objectives, "the pressures connected with surviving *[in this case external pressures]* can distort terrorists' ability to make rational decisions." [542]
- *Hypothesis: in certain cases (where groups are forced to hurry their planning or find their operational capabilities diminished) this may lead to less ambitious or strategically beneficial operational objectives. In other cases, if a group feels under pressure from their opponent and their capabilities are not substantially curtailed, a group may feel the need to assert their continued relevance or strike back at the enemy (punitively or to decrease his capability or distract him).*
- Higher profile attacks generally lead to less group security (McCormick[543]) and this is likely to factor into a group's calculation of its operational objectives.

General Planning Characteristics affecting Operational Objectives

- Decision maker Time Horizon
    - The general time horizon of decision makers can affect both the scale and type of attack chosen during the determination of operational objectives. Some decision makers, viewing themselves as the vanguard of a long, historical struggle (such as certain Marxists), may be more content to husband their resources and embark upon more modest actions at any point in time. However, decision makers working to a specific timetable (even when this is a self-imposed deadline, as in the case of certain apocalyptic groups), may feel the need to perpetrate more ambitious attacks, whether punitive or coercive in nature. Of course, heightened pressure from the security forces of a group opponent can lead to a sense of urgency as well. Both Post[544] and Pynchon[545] describe the causes and effects of a heightened sense of urgency and conclude that this increases the propensity for violence *(and by extension, in certain cases, for a greater scale of violence).*

---

[539] Post, Ruby, and Shaw, "The Radical Group in Context," p. 98.

[540] Hoffman, "Al Qaeda, Trends in Terrorism and Future Potentialities," p. 437.

[541] Pynchon and Borum, "Assessing Threats of Targeted Group Violence," p. 348

[542] Drake, *Terrorists' Target Selection,* p. 35. [Evidence Type: 1]

[543] "The set of all optimal operating points over a given time period defines its "tactical path." A terrorist group, by definition, cannot improve its performance as long as it can identify and stay on its tactical path. Any effort to improve its political position by increasing its operating profile, at this point, will be more than offset by a loss in security." McCormick, "Terrorist Decision Making," p. 497. [Evidence Type: 4]

[544] Post maintains that, "if a group feels that it will be in danger in the near future, it may be more likely to engage in terrorism due to a decrease in the range of perceived options. A group may be more likely to attack if it perceives a threat to group members or leaders, feels that the regime or other opponent is trying to destroy it, or becomes paranoid and defensive and attacks suspected traitors." Post, Ruby, and Shaw, "The Radical Group in Context," pp. 94-95. [Evidence Type: 2]

[545] Pynchon and Borum, "Assessing Threats of Targeted Group Violence," p. 348. [Evidence Type: 1]

- Risk Tolerance
  - *Hypothesis: The degree of risk that a group is willing to take to conduct any single attack is an important factor in the setting of operational objectives. All else being equal, the greater the risk tolerance of a group when planning an attack, the greater the scale of the attack is likely to be. A corollary to this is that the more wedded the group is to the success of an attack and group preservation (i.e., the lower its risk tolerance), the more conservative its operational objectives become. Risk tolerance is a function of the group's ideology and the external environment, among other variables.*

Attack Modalities affecting Operational Objectives

- Palfy stresses the importance of the order in which elements of an attack are determined and states that "selecting a particular weapon system *prior* to selecting a target, will have a significant bearing on the planning and overall outcome of an operation" (emphasis in original).[546] [Evidence Type: 1] Palfy does not, however, specify the manner in which planning is affected. Nonetheless, pre-selecting a particular weapon system can occur if, for example, a group's ideology mandates the cleansing of society through a biological agent, although this is likely to be a relatively rare occurrence. If it does occur, it can have the effect of limiting the group's operational objectives to those that can be achieved through the use of the pre-selected weapon.

Life Cycle affecting Operational Objectives

- Thornton states that attacks to get attention and recruit supporters and members (in the terms of the current model, symbolic organization-building attacks) are most common in the early stage of a group's operations, and that later on in a group's life-cycle these tactics are not expected to be as important as groups become more likely to engage in something closer to guerilla or symmetric combat. [547] Although Thornton admits that in most cases the shift to regular warfare does not occur, the above theory can today only be regarded as valid in an extremely limited context (for example, with some Marxist groups). There have been several recent cases where groups have eschewed limited, organization-building actions and jumped directly to desiring mass-casualty, apocalyptic-style attacks.
- Hoffmann[548] contends that in terrorist groups that survive long enough to spawn new generations of members, successor generations of a terrorist group or cause tend to be less idealistic, display a greater capacity for violence, and may even act expressively – all of which can impact elements of operational objectives such as desired casualty levels and the primary purpose of the attack.

Perceptual Filter affecting Operational Objectives

- Nothing noted in the literature reviewed. Perceptual filter will not affect operational objectives directly, but indirectly if it alters the perception of the flow of information from factors external to the group[549].

---

[546] Arpad Palfy, "Weapons System Selection and Mass-Casualty Outcomes," *Terrorism and Political Violence*, 15:2 (Summer 2003), pp. 87-88.

[547] "Thornton (1964), for example, suggested that actions designed to accelerate mobilization tend to diminish once this process is under way and the correlation of forces has begun to shift in favor of the rebels. "Agitational terror," he suggested, is particularly attractive (for the reasons we have just discussed) during the initial period of the conflict, when the opposition is trying to establish its *bona fides*…If all goes according to plan, the importance of these tactics can be expected to decline as the conflict takes on the characteristics of a force-on-force competition between the state and an increasingly regularized opposition." McCormick, "Terrorist Decision Making," p. 485. "Is it enough to argue that terrorist groups may not always make the best choices but that they at least attempt to do so? The answer to these questions is typically "no." If all does not go according to plan, which is typically the case, the group in question may never succeed in evolving beyond its use of agitational terrorism" *Ibid*. [Evidence Type: 1]

[548] "Not only are successor generations smarter than their predecessors, but they also tend to be more ruthless and less idealistic. For some, in fact, violence becomes almost an end in itself—a cathartic release, a self-satisfying blow struck against the hated "system"—rather than being regarded as the deliberate means to a specific political end embraced by previous generations." Hoffman, *Terrorist Targeting*, p. 5. [Evidence Type: 3]

[549] See discussion of the perceptual filter.

Capabilities Analysis[550]

The previous look at operational objectives provided the initial limitation of the target set. The following capabilities threshold analysis determines whether the group possesses or can obtain access to the resources and operational capabilities required to successfully perpetrate a major attack against critical infrastructure (as well as other types of attacks). It must be emphasized, however, that at this stage of the target selection process, the terrorist group has not yet narrowed its focus to any particular target,[551] and so will evaluate their capabilities in a general sense. In other words, at this stage in the process they will be asking themselves "Do we have the capability to even consider attacking target type X?" rather than evaluating their capability to attack a specific site or facility.

This stage of the analysis is particularly demanding for two reasons:

1) *There is no single set of capabilities required to attack critical infrastructure; indeed, the operational capabilities and resources needed to inflict serious damage may differ significantly from one type of infrastructure to the next (and of course from one specific target to the next), making any generalization difficult.*

This is dealt with by listing (to the extent possible) the minimum requirements for each specific infrastructure type, based on the historical record[552]. If the other areas of the analysis have given any indication of a particular type of infrastructure that the group may be drawn towards (for example, if the group leader has a background in aviation) or if only certain types of infrastructure are available in the group's area of operation, the capabilities assessment can be limited to these specific infrastructure types. See Table 5.2 on the page after next and the accompanying explanation of variables for a listing of the required capability levels needed historically to achieve a high impact.

Since one of the primary determinants of required resources is the level of protection of the infrastructure, the table lists the results for both high and low levels of protection. In many cases, there are no records of attacks against sites with a certain level of protection: these are excluded. In other cases, there were no high impact attacks recorded, and therefore the requirements for low impact attacks have been substituted (and indicated in the table by italics).

If, however, there is no indication that any particular infrastructure is more vulnerable or more attractive to the group under consideration, then the most that can be done is to compare the group's capabilities against the 'lowest common denominator'[553] of all CI target types, which sets a baseline for required levels of capabilities and resources. This is indicated in Table 5.2 under the category GENERAL. Of course, if one is evaluating a specific target, one should use the data for that particular target, which can be determined from a vulnerability study.

---

[550] In this section 'capabilities' refers to both resources and operational capabilities.
[551] This occurs at a later stage of the process, and is not the focus of the framework, which is to assess the intent of terrorists to attack general critical infrastructure targets, and if possible the type of infrastructure selected, but not the specific target itself.
[552] The project team looked at all high impact cases in CrITIC in each infrastructure category, noted or estimated the required levels of capabilities and resources used, and averaged these. The complete list of case analyses is available from the authors.
[553] Since the required operational capabilities and resources for attacking the Oil/Gas infrastructure are uniformly low, this was excluded in order not to bias the results (with the caveat that if the Oil or Gas infrastructure is a potential target, special attention needs to be given to this area).

2) *Analysts do not only have to consider whether the group could actually attack critical infrastructure (although this is a significant part of the larger threat assessment), but rather whether or not the group itself perceives that they have this capability. Even where a group does possess the requisite capability, if it does not perceive this to be the case, it will refrain from attacking. On the other hand, even unsuccessful attacks by groups who believed themselves capable have sometimes proven to have deleterious consequences.*

This complication is somewhat more difficult to address in that it deals with the effect of group perceptions, which (as mentioned previously) is an extremely difficult element to assess. We feel that the best way to deal with this given current tools is to assume, at least in this aspect of decision making, that any moderately competent terrorist group will be able to evaluate its capabilities more or less accurately, and that any group considering a large-scale attack will do enough homework to have at least some idea of the capability levels required to attack various targets. Those groups whose evaluation is consistently off the mark will probably not remain viable for long. That being said, the analyst should use whatever information she has about the group's perceptual biases in order to attempt to determine how far and in what direction the group's perception of their own capabilities and those required to perpetrate an attack can be expected to differ from more objective evaluations of these measures.

Once the required capabilities have been determined, the following flowchart can be consulted using Table 5.2 together with all information collected or inferred thus far. To save space, the phrase "in the group's perception" has been omitted, but applies to the entire chart[554].

[554] The chart reflects the notion that once terrorists have determined their general operational objectives, or perhaps once they have decided that a certain target or class of targets is attractive, they may find that they lack the requisite resources to engage in the type of attack that would give them the effects they seek. This can, under certain circumstances, prompt the group to build up their resources to the levels and types required to perpetrate the desired type of attack. The extra resources can be achieved through, *inter alia*, purchase, theft, indigenous development or transfer from an external supporter. The circumstances under which this will apply are governed by such factors as the decision makers' time horizon, their ideological or idiosyncratic attraction to a particular target, or the lack of alternative targets yielding the same level of perceived gains (as elucidated in other parts of the model).

Table 5.2 Capability Requirements for Attacking Specific CI

Infrastructure Type	Protection Level	Physical Resources	Weapons	Financial Resources	Logistical Resources	Ability to innovate	Technology level	Skill set (esp. military-type skills)	Familiarity with Target Environment	Communications
Aviation Infrastructure	High	High	Medium	Low	Medium	Medium	Medium	High	High	Medium
	Low	Medium	Medium	Low	Medium	Low	Medium	Medium	Medium	Unknown
Chemical Plant	Low	Medium	Low-Medium	Low	Medium	Medium	Medium	Medium	High	Medium
Communication Infrastructure	Low	Low	Low-Medium	Low	Low	High	High	Medium	High	Unknown
Dams and Waterways	Low	Medium	Unknown	Low	Unknown	Unknown	Medium	Medium	High	Unknown
Embassies/Consulates	Low	Low	Medium	Low	High	High	Medium	High	Medium	High
Financial Institutions	High	Medium	Medium	Low	Medium	Medium	Medium	Medium	High	Medium
	Low	Low-Medium	Medium	Low	Medium	Medium	Medium	Medium	High	Medium
Police Stations *(low impact only)*	*High*	*Medium*	*Medium*	*Low*	*Unknown*	*Unknown*	*Medium*	*Medium*	*Unknown*	*Medium*
Oil/Gas Infrastructure	Low	Low	Low	Low	Low	Low	Low	Low	High	Low
Power Infrastructure	Low	Medium	Medium	Low	Medium	Medium	Medium	Medium	Medium-High	Medium
Public Service/ Government Office	High	Medium	Medium	Low	Medium	Medium	Medium	Medium	High	Medium
	Low	Medium	Low-Medium	Low	Medium	Medium	Medium	Medium-High	Medium-High	Unknown
Military Bases	High	High	Medium	High	Medium	Medium	Medium	Medium	High	Medium
Railways/Railroads/Rail lines	Low	Medium	Low-Medium	Low	Medium	Medium	Medium	Medium	High	Medium
Roadways *(low impact only)*	*Low*	*Medium*	*Unknown*	*Low*	*Unknown*	*Unknown*	*Medium*	*Unknown*	*Medium*	*Unknown*
Subways	Low	Medium	Medium-High	Low-High	Medium-High	Medium-High	Medium-High	High	High	Medium
Train/Bus Stations	Low	Medium	Medium	Medium	Medium	Medium	Medium	High	High	Medium
Water Treatment/ Storage Facility *(low impact only)*	*Low*	*Low*	*Low*	*Low*	*Unknown*	*Unknown*	*Low*	*Unknown*	*Unknown*	*Unknown*
GENERAL	HIGH	MEDIUM	MEDIUM	LOW	MEDIUM	MEDIUM	MEDIUM	MEDIUM	HIGH	MEDIUM
	LOW	LOW	LOW-MEDIUM	LOW	LOW	LOW	MEDIUM	MEDIUM	MEDIUM	MEDIUM

Physical Resources (equipment, vehicles, etc.):
High: Plentiful vehicles, sophisticated equipment
Medium: Standard equipment, some vehicles
Low: Basic, minimal equipment

Weapons:
High: Sophisticated conventional explosives, WMD
Medium: Large-scale simple conventional explosives
Low: Small-scale IEDs, guns, mortars, grenades

Financial Resources:
High: >$50,000 available to carry out any attack.
Medium: $10,000 – $50,000 available to carry out single attack
Low: <$10,000 available to carry out attack

Logistical Resources *(safehouses; fake passports etc.):*
High: Vast: Competent logistical network with high redundancy
Medium: Some safehouses and logistical competence
Low: Minimal support network; difficulty coordinating anything other than basic attack

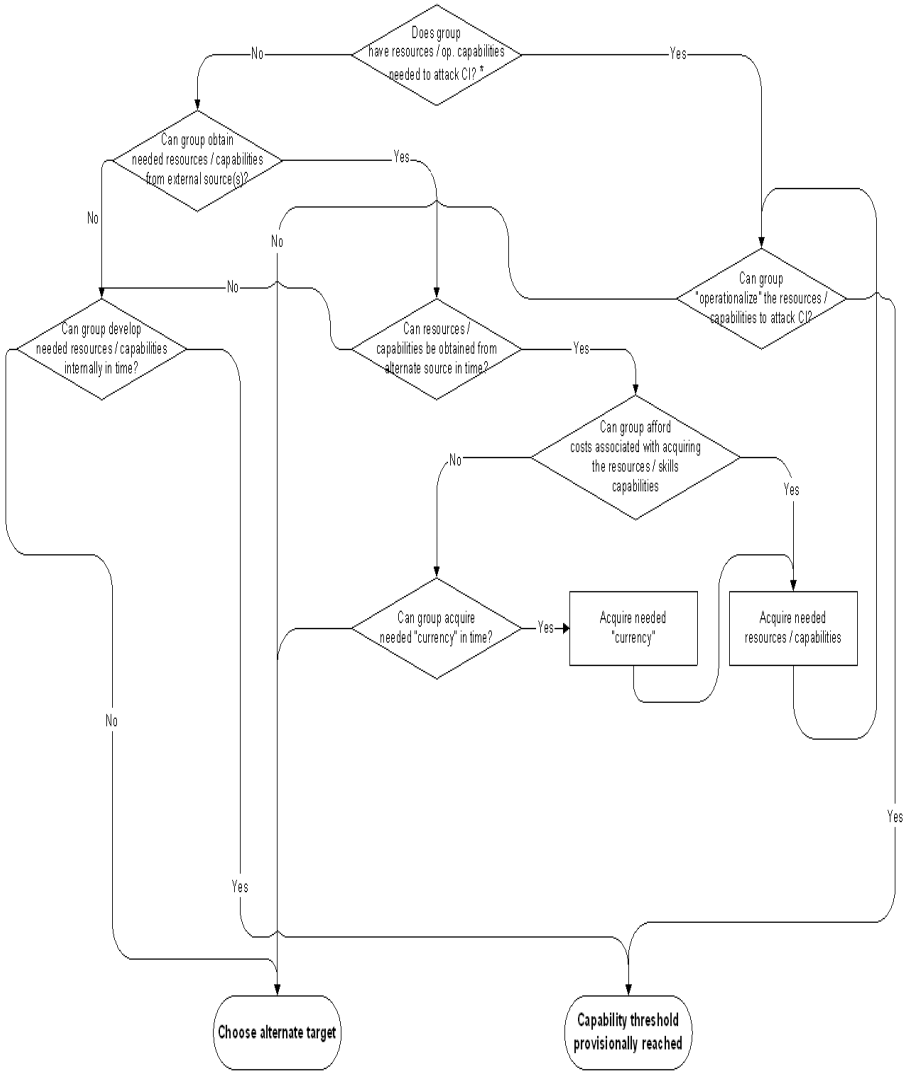
Ability to innovate:
High: Easily embraces new technologies and techniques; quickly gains tacit knowledge
Medium: Competent at adopting new technologies and techniques, although not a particular strength
Low: Difficulty adopting new technologies or techniques

Technology level:
High: High technical skill; aware of and capable of using newest technologies
Medium: Standard technological level – commercial off-the-shelf technologies
Low: Only rudimentary equipment and techniques – low-tech only

Skill set (esp. military-type skills):
High: Highly trained members with diverse relevant skills (e.g. explosives production, electronics)
Medium: Some paramilitary type training, basic tradecraft
Low: Amateurish, little to no formal training

Familiarity with Target Environment:
High: Intimately familiar with target environment, can blend in easily
Medium: Some familiarity with target environment, but not perfect
Low: Unfamiliar with target environment – easily noticeable

Communications:
High: Robust and extensive communications networks
Medium: Workmanlike communications capabilities but no redundancy
Low: only primitive, limited-channel communications possible



* This is determined by comparing the relevant row (either a specific infrastructure or General) in Table 5.2 with the known resources and capabilities of the group (collected from intelligence or inferred previously in the framework)

The above analysis should enable the analyst to provide at least an initial assessment of the group's perceived capabilities vis-à-vis a large-scale attack on critical infrastructure.

In order to confirm this analysis, or in cases where information is just too sparse to utilize the above tools, the analyst should now revisit their earlier analysis and collect all the 'C' (capability) indicators yielded by the factor analysis process. These are much more general than the above analysis and capture factors that are expected to increase or decrease the terrorists' perceived capabilities to attack critical infrastructure. The 'C' indicators can be amalgamated (by the process described below) to yield preliminary indications of perceived capabilities derived from an alternative avenue of analysis and can either confirm the above perceived capabilities threshold, argue for analyst reevaluation (if it contradicts the above results), or provide an alternative explanatory mechanism if there is insufficient data to conduct the above analysis.

The Special Case of Insiders

Insiders can dramatically alter the operation of the above section of the framework. There are two cases where an insider is used:

a) Once the target has been selected, the group inserts an insider into the target facility – in this case, the use of an insider forms part of the attack modalities (roughly the tactics used) and does not affect the above perceived capability analysis portion of the motivation assessment. Insiders in this case fall outside this framework.
b) Before the target has been chosen, the group already has an insider in a facility, or expects to be able to reliably insert one – in this case, the availability of an insider can have a large impact on target selection, to some extent obviating the abovementioned capability and resource requirements and making it especially likely that the group will select that target over one where gaining access is more difficult. As Schneier remarks, "Insiders might be less likely to attack a system than outsiders are, but systems are far more vulnerable to them. An insider knows how the systems work and where the weak points are. He knows the organizational structure, and how any investigation against his actions would be conducted. He may already be trusted by the system he is going to attack. An insider can use the system's own resources against itself. In extreme cases the insider might have considerable expertise, especially if he was involved in the design of the systems he in now attacking."[555]

Preliminary Target Selection: Putting the Pieces Together

The final stage in the analysis is in some respects the simplest and in others the most difficult. It is simplest in the sense that all the work has already been done – all that remains is for the analyst to combine the various analytical elements to arrive at some conclusions about the group's proclivity for choosing to attack critical infrastructure. On the other hand, this can be the most difficult step, since the act of combination requires all the creative skills of the analyst and harbors several potential pitfalls. In some respects this is the point at which the 'art' of analysis comes to the fore.

Our framework divides the target selection process into the three stages[556]:

1) **Preliminary Target Selection:** The terrorists choose a type of target (or perhaps a specific target) that they would like to attack (based on all the factors discussed thus far and their general perceived capabilities). In principle, the terrorists perceive the members of this target set[557] as equally attractive at this point, and they consider themselves capable of attacking any one of them. It is at this stage, for example, that the terrorists might decide to attack an oil refinery, or a bank in a city center, or a crowded marketplace.

---

[555] Schneier, *Secrets and Lies*, p.48.

[556] Anecdotally, these stages are described by an unidentified American left-wing radical who describes the process as follows: "The 'first decision', he said is … political—determining appropriate and possible targets. Once a set of targets is decided on, they must be reconnoitered and information gathered on how to approach the targets, how to place the bomb, how the security of the individuals and the explosives is to be protected. Then the time is chosen and a specific target."

[557] In many cases, the target set may contain only a single member. Hoffman, "The Modern Terrorist Mindset: Tactics, Targets, and technologies," p. 13.

2) **Surveillance and Intelligence Gathering:** The terrorists proceed to actively begin to gather intelligence on a specific target or set of targets that fall within their desired target and attack type.

3) **Final Target Selection:** After collecting 'on the ground' data about the targets of interest, such as specific security arrangements surrounding the target or access routes to and from the target, the terrorists select or confirm the single target that offers them the greatest chance of success. If the targets reconnoitered in stage 2 are all unsuitable because of tactical-level constraints, the terrorists must begin their decision process again (or at least several factors of the process) in order to select an alternative target.[558]

Since the surveillance and final target selection stages depend on a variety of tactical level observables and criteria that are almost wholly dependent on specific target site characteristics, they do not lend themselves to a general motivational analysis such as this to any appreciable degree. The surveillance and final target selection stages involve a whole new set of factors and indicators that move beyond the current framework. The current analysis will therefore conclude at the preliminary target selection stage, which we feel still yields a significant operational advance over previous attempts to elucidate targeting decisions.

At this final stage of the journey through the DECIDe framework, the analyst must consider carefully the nexus between the terrorist group's operational objectives, their perceived capabilities[559] and the attractiveness to key decision makers of attacking a critical infrastructure target.

These must all be considered relative to the characteristics of critical infrastructure targets. In reality there is no simple relationship here.[560] For instance, in the case of the influence of target characteristics such as level of protection, targets that are generally perceived to be more vulnerable and have a higher impact loss are likely to be more attractive to terrorist groups, all else being equal. However, all else is not always equal. A group seeking the simplest way to gain attention for their cause may be deterred by the level of protection surrounding a nuclear power plant. However, another group that has high technical capability and resources, high risk tolerance and is in competition with a rival group for supporters, may particularly seek out such well-protected targets as an opportunity to demonstrate its strength and capabilities to potential recruits (or perhaps just its commitment and courage, in which case the 'success' of the attack in terms of physical disruption or destruction becomes less crucial).

In this case, analysts should compare and weigh the characteristics of the target (or class of targets) with both operational objectives and general capabilities and then consider the attractiveness of a critical infrastructure target in relation to these factors.

---

[558] Their decision making would now necessarily include a revised estimate of their capabilities to attack certain targets, following their inability to attack any of their preferred targets from the preliminary target selection stage.

[559] It must be remembered, however, that even if a group knows it lacks the capability to carry out a successful attack, for certain objectives, even an unsuccessful attack may suffice. For example, a leader whose members are becoming restless may, for organization building purposes, plan an attack simply for the purpose of giving them something to do. It can be assumed that attacks based solely on these considerations would be fairly rare.

[560] See Chapter 2 for a detailed discussion of the effect of target characteristics on target selection.

The following steps elucidate this process and utilize both analytical mechanisms found in the framework:

1) Evaluate the restricted target set determined during the previous stage in the analysis (reflecting both operational objectives and perceived capabilities). Are any critical infrastructure targets still within this truncated set? If not, the chances of the group selecting a critical infrastructure target are extremely slim.

2) Assuming critical infrastructure targets are still within the restricted target set, are there any factors that make attacking a critical infrastructure target especially attractive? This can be answered by collecting up all the 'A' (attractiveness) indicators yielded during the factor analysis process. One may be tempted here to use a simple arithmetic approach, to list all the pluses and minuses, determine which cancel each other out and arrive at a simple 'mathematical' solution. This is not at all the intended approach of this framework. Rather, analysts are urged to look at each 'A' indicator, understand the conditions in which it arose, i.e. which particular factor led to its value and under what circumstances and to what extent that factor holds, and thereafter to evaluate the collection of factors in the context of all the known group information. Also, the attractiveness values need to be considered, not in isolation, but relative to the attractiveness of other target and attack types[561]. Careful and thorough consideration of the attractiveness indicators can lead to conclusions about whether critical infrastructure targets would be more attractive to terrorist decision makers than other targets at a particular point in time.

3) The final element of the analysis is for the analyst to assess whether any influences not already taken into account could modify the conclusions reached in the previous step. These could include specific group dynamics or perceptual distortions that occur specifically at the target selection stage and that have not already been accounted for at other stages of the analysis.

Upon completion of the above steps, the analyst should at the very least be able to articulate the various reasons why a group would or would not select a critical infrastructure target and how they view these targets in relation to others. As mentioned previously, we are not asserting that terrorist decision makers follow this framework in their decision making – in fact, many of the intervening factors may operate unconsciously and it is doubtful that the mental processes of any human decision maker, let alone a terrorist, will explicitly resemble the above framework. Rather, the framework is an aid to organizing and elucidating the complex and intricate process involved in target selection, with specific application to the question of how likely the ultimate target is to fall within the category of critical infrastructure.

The worksheet provided as Appendix II can be used to aid analysts as they work through the DECIDe Framework.

[561] Most of the 'A' factors in the framework have been consciously constructed to implicitly assess critical infrastructure relative to other target and attack types. However, this aspect should still be borne in mind during the final evaluation.

A Few Words on Attack Modalities

Attack modalities are directly relevant to answering the question of how terrorists would conduct an attack on critical infrastructure. While the focus of this study is squarely on the "why" as opposed to the "how", and the DECIDe Framework does not deal at all with the decisions taken subsequent to target selection, several notable observations relating to attack modalities emerged during the research for this study and are mentioned here in passing in the hope of stimulating further research. Firstly, the case studies of Chukaku-ha and the Indian Parliament attack gave some idea of the approaches taken by terrorists in attacking Critical Infrastructure, while the CrITIC Database confirmed the common-sense notion that most attacks against CI would make use of explosives. Lastly, the influence of various factors on attack modalities was extracted from the literature, the most important of which are listed below.

Factor Influence List: Attack Modalities

Operational Objectives affecting Attack Modalities

- Operational objectives can determine whether an attack is OVERT or COVERT (in the sense of revealed as an intentional attacks or not), as implied by Schneier[562] [Evidence Type: 1]. *Hypothesis: symbolic attacks will be overt (at least eventually), while purely instrumental attacks need not be.*
- Operational objectives will mostly determine the WEAPON TYPE USED:
    - Palfy alleges that when terrorists want to reliably cause mass casualties, conventional weapons will be used; when fear and disruption *irrespective of casualties* is desired, terrorists may be more tempted to use unconventional weapons[563] [emphasis added].
    - Palfy also argues that "The relationship between the desired outcome [in our nomenclature, operational objectives] and terrorist weapon selection therefore supercedes other aspects of a given terrorist operation,"[564] and "By accounting for both the weapon-target and intentions-outcomes relationships, it becomes possible to theoretically determine the best-suited weapon system for a specifically desired outcome."[565]
    - Jackson (and several others) aver that groups seeking punitive effects could consider using weapons of mass destruction, "…a group seeking maximal

---

[562] "Specific attacks range from subtly modifying systems so that they don't work (or don't work correctly) to blowing up systems completely. The attacks could be covert, in which case they might resemble terrorist attacks (although a good infowarrior cares less about publicity than results)." Schneier, p.57.

[563] "…[M]issions and groups specifically seeking to produce large amounts of casualties will prefer employing conventional weapons systems, while others predominantly focusing on inciting fear, panic and general disruption—regardless of the amount of resultant casualties, may be more tempted to use unconventional weapons," and "…the use of unconventional weapons is largely dependent on the terrorists' desired mission outcome. That is to say, missions *specifically* seeking to cause large amounts of casualties, even if only as a means to a desired end, will tend to employ weapons of a more conventional nature, though will perhaps do so in more elaborate ways. Conversely, terrorist missions seeking to disrupt, intimidate, or otherwise interrupt the regular functioning of a state, *irrespective* of total casualties or fatalities produced, may be tempted to employ chemical and biological-type weapons" and ""…seeking a greater number of casualties per incident may incite an alteration in the types of targets and tactics selected, but not necessarily in an alteration of the weapon systems employed against them (i.e., CBRN-type weapons instead of conventional ones)." Palfy, p.81–82, p.91. [Evidence Type: 1]

[564] Palfy, p. 82. [Evidence Type: 1]

[565] Palfy, pp. 86-87. [Evidence Type: 1]

destruction for the benefit of a divine audience would likely conclude such destructive weapons would be appropriate to their goals."[566]

- In addition to escalating the lethality and scale of attack, another way in which a group could garner more media attention is to conduct a particularly sophisticated or technologically complex operation.
- Jackson argues that the sophistication of terrorist operations increase as they strive to escalate the scale and lethality of attacks in order to gain attention and influence target audiences.[567](Evidence Type: 1)

Ideology affecting Attack Modalities

- *Hypothesis: Depending upon their ideological precepts, certain groups seem to be more inclined to utilize highly destructive weapons. This will in turn affect their attack modalities.*
- Ideology also plays an important role in determining the choice of weapons and the choice of tactics employed in terrorist actions.[568] [Evidence Type: 1]

Resources affecting Attack Modalities

- Advances in information technology and exchange of information have allowed terrorists to propagate successful attack techniques and tools. This medium of accelerated knowledge transfer has reduced the need for training and increased the operational capability of terrorists.[569] [Evidence Type: 1]
- According to Drake the size of a group affects the complexity of attacks it can conduct.[570] [Evidence Type: 1]
- According to Woo, "off-the-shelf-weapons" are attractive to terrorists for their past record of success.[571] [Evidence Type: 1]

Operational Capabilities affecting Attack Modalities

- Hoffman provides evidence to argue that a vast majority of terrorists are not tactically innovative but rather, employ tried and tested tactics.[572] [Evidence Type: 1]

Critical Infrastructure (CI) Characteristics on Attack Modalities

- Hoffman suggests that terrorists gather information regarding their target to gather information on how to approach the targets, how to place the bomb, how the security of the individuals and the explosives is to be protected.[573] [Evidence Type 1]
- Drake also asserts the importance of target characteristics in determining the operational planning for an attack. He states that terrorists need to know the level of protection in order to estimate the degree of force needed to overcome any protective security.[574] [Evidence Type 1]
- The level of security at a CI facility is a very important factor that plays a role both in the selection of targets and in planning the operational level of attack. An increase in the security level for a facility might force terrorists to invest more time and money to overcome the increased security measures.[575] [Evidence Type: 1]

---

[566] Jackson, "Technology Acquisition by Terrorist Groups," p. 190. [Evidence Type: 1]

[567] Jackson, "Technology Acquisition by Terrorist Groups," p. 185.

[568] Hoffman, "The Modern Terrorist Mindset," p. 1

[569] Schneier, *Secrets and Lies*, pp. 20-22.

[570] Drake, *Terrorists' Target Selection*, p. 88.

[571] Gordon Woo, "The al-Qaeda War Game: Following the Path of Least Resistance," Risk Management Solutions, Inc., (December 2002).

[572] Hoffman, *Terrorist Targeting*, p. 2

[573] Hoffman, "The Modern Terrorist Mindset," pp. 13-14.

[574] Drake, *Terrorists' Target Selection*. p. 111.

[575] *Ibid.*

- Jackson points out that increased security measures might lead terrorists to adopt highly damaging tactics to overcome such protective mechanisms. As an example, Jackson cites that terrorists might use a guided missile to destroy a highly protected airport which is impregnable by vehicles or human agents.[576] [Evidence Type: 1]
- The location of a target relative to the terrorists' base might affect the operational planning for a particular attack. According to Woo, the location of a target that is not in the same area as that of the terrorists' base might lead the terrorists to use off-the shelf weapons systems and delivery systems for carrying out a particular attack.[577] [Evidence Type: 1]

According to Palfy, terrorist techniques become less complex when operating in an unfamiliar theater. Thus, the need for operations to be simple in unfamiliar environments.[578]
[Evidence Type: 4]

[576] Jackson, "Technology Acquisition by Terrorist Groups," p. 183-213.
[577] Woo, "Understanding Terrorism Risk," p. 14.
[578] Palfy, "Weapons System Selection and Mass Casualty Outcomes," p. 87.

Chapter 6: CONCLUSION*

A. Approach

This research effort set about trying to answer some basic but complex questions about terrorist target selection, specifically in the context of potential future attacks against the nation's critical infrastructure. The CNS research team employed a number of different investigative approaches in this study, and sought to exploit the synergy between them in order to "operationalize" its findings. Among the methods that were adopted to shed light on this topic were: 1) a review of existing terrorism and threat assessment literature to both glean expert consensus regarding terrorist target selection and identify theoretical approaches that might be valuable to analysts and decision-makers who are seeking to understand such terrorist group decision-making processes; 2) the preparation of several concise case studies to help identify internal group factors and contextual influences that have played significant roles in leading some terrorist groups to attack critical infrastructure; 3) the creation of a new database – the Critical Infrastructure Terrorist Incident Catalog (CrITIC) – to capture a large sample of empirical CI attack data that might be used to illuminate the nature of such attacks to date; and 4) the development of a new analytical framework – the Determinants Effecting Critical Infrastructure Decisions (DECIDe) Framework – designed to make the factors and dynamics identified by the study more "usable" future efforts to assess terrorist intentions to target critical infrastructure.

Even though these four components of the study are presented separately in this report, none of them were developed in isolation. Rather, all the constituent elements of the project informed – and were informed by – the others. For example, the review of the available literature on terrorist target selection made possible the identification of several factors that were later validated by the case study analyses. Similarly, statistical analysis of the CrITIC data yielded measurable evidence that supported the conclusions utilized in the analytical framework.

Besides providing an important mechanism of self-reinforcement and validation, the project's multifaceted nature made it possible to discern aspects of CI attack motivations that would likely have been missed if any single approach had been adopted. For example, CrITIC – which was created specifically for this project – reveals important macroscopic information about the nature and general patterns of CI attacks during the last several decades. Since this information is not available in any other single source outside the classified realm, CrITIC facilitated a better understanding of historical trends in attacks on CI, such as the relative frequency with which different categories of terrorist groups have attacked critical infrastructure; the relative frequency with which different categories of critical infrastructure have been attacked; the relative frequency with which different tactics and tools (e.g., weapons) have been employed to attack critical infrastructure; and the relative impact – in terms of casualties – associated with different attack types, different terrorist group types, and different CI target types. By cataloging past CI terrorist attacks and controlling the data for different variables, we were able to ask increasingly sophisticated research questions and thence determine preliminary answers to them using statistical methods.

* This chapter was written by Gary Ackerman, Jeffrey M. Bale, and Kevin S. Moran.

The case study component of the project, on the other hand, enabled the research team to consider a select number of distinct but in certain respects representative examples of critical infrastructure attacks in much greater detail and with much more specificity. While our analyses of these cases yielded conclusions that broadly conformed to those generated by other parts of the study, it also provided insight into the harder to quantify factors and dynamics influencing terrorist target selection. Hence the case studies offered a much better understanding, both of the contexts in which such attacks were made and the ways in which terrorist motivations have been shaped by powerful internal forces such as ideology, operational objectives, operational capabilities, organizational structure, social dynamics, and perceptions of external realities (e.g., the overall security environment and the specific characteristics of potential targets).

Although the survey of the existing literature uncovered little that specifically addressed terrorist motivations for attacking critical infrastructure, it provided a wide range of contextual and genre-specific material that enabled us to more firmly relate this project to the broader body of contemporary terrorism research. The literature assessment proved to be particularly valuable in aiding efforts to produce a decision-making framework that captures as fully as possible the factors and dynamics integral to terrorist target selection. Similarly, the framework development process consistently raised vital research questions that were subsequently explored in the study's other research tracks.

B. Key Findings

The study's key conclusions are best highlighted and understood in the framework of the original four research questions that were posed at the outset of this study, in Chapter 1.

I. Why do terrorists attack critical infrastructure rather than other targets?

There is any number of possible reasons why terrorist groups may decide to attack CI, some of which are the same as their reasons for attacking other types of targets and some of which are due to the intrinsic or peculiar characteristics of CI. The simplest and most obvious reason, which clearly falls into the intrinsic category, is that terrorist groups will attack CI for strictly pragmatic "infrastructural" reasons, i.e., in order to disrupt or interrupt the functioning of certain key facilities, the damage or destruction of which will seriously impinge upon the normal operation of a given society. Al-Qa`ida members have explicitly listed this as being one of their group's primary objectives, all the more so when attacking industrialized countries like the U.S. and those in Europe, where attacks on critical facilities are likely to have both a tangible, cascading effect on integrated infrastructural systems and a tremendous psychological impact on populations accustomed to enjoying their conveniences and creature comforts.

A second reason is that certain terrorist groups may have an ideological predilection to attack CI because they see various infrastructural entities as embodying the very "injustices" they are trying to redress. This is the main reason why the FLNC attacked infrastructural targets on Corsica. Third, other groups may attack CI because infrastructural targets have a particularly resonant symbolic value as well as a potentially extensive impact. For example, the main reason that the FARC attacked power generating facilities and oil pipelines was to interrupt basic services so as to display the impotence of the Colombian government. Fourth, still other groups may do so in order to rally or express their solidarity with their proclaimed constituents, in particular those on whose behalf they purport to be fighting. This is clearly one of the primary

reasons why Chukaku-ha attacked the JNR. Fifth, some groups may do so because they are seeking to obtain maximum publicity *without* causing large numbers of casualties, as is probably the case with the MILF, whereas others may attack certain CI precisely because they wish to inflict mass casualties on their enemies, as is surely the case with various global jihadist networks.

However, in many if not most cases, it is probable that terrorist groups will decide to attack infrastructural targets for a multiplicity of reasons rather than for only one reason, as the examples of the 9/11 attacks, the 1993 World Trade Center bombing, and the assault on the Indian Parliament suggest. In sum, it is probably safe to conclude that terrorists generally attack infrastructure because: 1) they want to destroy certain important facilities; 2) they feel that they can obtain more publicity or external support than if they had attacked non-infrastructural targets; 3) they can cause even larger number of casualties – or avoid causing casualties altogether – by attacking such facilities; 4) the symbolic value of infrastructural targets is greater than that of other targets; or 5) for a complex combination of general and very specific reasons. As one would expect, there is no single explanation that is applicable to all the prior cases of attacks on CI.

II. Which types of critical infrastructure do terrorists prefer to attack?

With regards to the types of infrastructure attacked and the methods of attack, of the confirmed *major* CI attacks between 1933 and 2003, Oil/Gas, Power, and Public Service/Government Office infrastructure facilities were targeted most frequently. As is discussed in more detail below, attacks on Oil/Gas Infrastructural targets also accounted for the largest number of casualties. However, if one includes minor attacks against CI, attacks on Embassies/Consulates accounted for almost 50% of the total, even though they incurred a negligible number of fatalities when compared to attacks on other CI categories. Bombing has been the most favored method of attacking CI, but given that most of the bombing types are unknown, further research would be required to give these numbers more specificity.

Between 1933 and 2004, 50% of the major attacks against CI were against Oil/Gas Infrastructure. As far as other *major* attacks are concerned, Power Infrastructure targets amounted to about 15%, followed by Public Service/Government Offices (8%), Railways/Railroads/Rail lines (5.3%), and Dams and Waterways (3.7%).

As for terrorist group types involved in CI attacks, the largest number of confirmed *major* attacks against CI was carried out by Secular Utopian groups, with 47 attacks, almost all of which were Marxist groups. During the same period, Ethno-Nationalist groups carried out 43 major CI attacks, and Religious groups carried out 19. However, the overall percentage of Religious group attacks on infrastructure has increased significantly in the past decade and a half. Secular Utopian and Ethno-Nationalist groups have both displayed a propensity to attack Oil & Gas infrastructure facilities, which constituted more than 50% of their total number of major infrastructure attacks. In contrast, Religious groups made major attacks against various types of infrastructure.

More than 50% of the *major* attacks on CI in Europe and Latin America/Caribbean were carried out against Oil/Gas Infrastructure. Significantly, in the Middle East/North Africa region, the attacks on Oil/Gas Infrastructure accounted for almost 85% of the attacks on CI. The high percentage of attacks on CI in this region could be partly attributed to the vast number of oil and

gas infrastructure targets in the region, as well as to the vulnerability of those targets vis-à-vis other CI. In contrast, in Asia the attacks on Oil/Gas Infrastructure amounted to only 30% of the major attacks on CI.

The data for *major* attacks on CI indicate that terrorists have targeted Oil/Gas Infrastructure most consistently since 1960. In every decade beginning with the 1960s, the number of attacks on Oil/Gas Infrastructure has been higher than the number of attacks on other types of CI.

III. What types of groups are most likely to attack U.S. critical infrastructure?

On the basis of past trends, other categories of terrorists (such as nationalist and secular utopian groups) have conducted the majority of attacks against CI worldwide. The absence of many of these group types in the U.S., however, and the increasing incidence of attacks by religious groups suggest that three main categories of terrorist groups may have the highest disposition to attack U.S. critical infrastructure targets in the future: 1) transnational Islamist terrorist groups, 2) domestic right-wing "militias," and 3) the most violent fringes of the radical ecology movement.

Global Jihadist Groups. Among the three groups that are most likely to want to conduct attacks against CI, Islamist terrorist groups possess both the ideological proclivities and the necessary operational capabilities to perpetrate large-scale CI attacks. Analysis of CrITIC Database incidents reveals that Islamist terrorist groups have significantly increased both the volume and lethality of their CI attacks during the past two decades. In terms of absolute numbers, groups generally classified as "Religious" have accounted for roughly 73% of all casualties and 35% of all fatalities for confirmed major CI attacks. If both major and minor attacks are included, the data reveal that these groups have accounted for 62% of all casualties, the vast majority of which fall into the "Islamic" subcategory. These statistics support a frightening hypothesis – that religious terrorist groups are more likely than other groups to mix CI attacks with mass casualty attacks.

Right-Wing Militia Groups. As discussed in the case study chapter, critical infrastructure might be expected to be an attractive target for certain domestic right-wing militia groups given their ideological and operational objectives. Several groups of this type have publicly expressed an interest in attacking CI as part of their struggle against the "New World Order" and the "Zionist Occupation Government," and some have even published treatises advocating the targeting of certain government facilities. Although militia-type groups have already attacked CI in the US, most of their attacks have not been particularly successful. The relatively unsophisticated organizational and operational capabilities of most of these paramilitary cells, along with their frequent infiltration by law enforcement operatives, have thus far generally inhibited their ability to carry out large-scale attacks on CI. (The only exception has been the 1995 Oklahoma City bombing, which for the reasons noted above does not clearly fall into the infrastructural category.) However, their oft-expressed interest in attacking infrastructural targets, and the ease with which certain types of CI attacks can be made, means that analysts and policymakers should not discount the threat that these groups might pose in the future.

Radical Ecology Groups. Fringe elements from certain radical ecology groups pose a threat to particular types of CI that are directly linked to their specific ideological agendas, such as scientific laboratories that engage in genetic or biotechnology research. Moreover, the growing intermixture and interaction between radical ecologists and anti-capitalist, "anti-globalization," and other social revolutionary activists presents a latent but potentially significant threat to

critical infrastructure in the U.S. Although such groups have often proclaimed their intent to avoid causing human casualties, the weakening of such restraints cannot be ruled out in the future.

In sum, although foreign nationalist and Marxist groups were the most prone to attacking CI from the 1960s through the 1980s, they are far less likely to attack infrastructural targets on U.S. soil in the near future than the types of groups enumerated above. If, however, Marxist or nationalist terrorist groups were to become active in the U.S. in the future, these would might be expected to pose a significant threat to CI.

IV. How do terrorists make decisions and plan to attack critical infrastructure?

The manner by which terrorist groups make targeting decisions is an involved process which necessarily varies somewhat from group to group, but in general one can characterize it as follows. First, a group's ideology, by explicitly indicating what the group is for and against, essentially establishes the range of possible human and non-human targets that its members can legitimately attack. This maximal range of targets is, in most cases, further limited by the group's specific operational objectives for launching a particular attack. Once those objectives have been determined, several targets will be identified that might enable the group to achieve its objectives. At that point the group will consider which of those targets can be successfully attacked given its own operational capabilities. A variety of factors that make CI targets particularly attractive may also be presented. After the potential range of targets has been further reduced and various specific targets have been identified in a preliminary way, the group will then conduct close surveillance to determine which of these are most vulnerable, i.e., which can likely be attacked successfully. After that determination has been made, a final target will be selected and additional information will be collected on the layout of the site, the configuration of the facility, its levels of protection, its peculiar vulnerabilities, approaches to and from the site, etc. When the group feels that it has acquired enough information on the target, it will develop a specific plan of attack and then launch the attack.

Obviously, this is a highly schematic overview of the general process, many phases of which are in fact likely carried out simultaneously. Moreover, in some instances certain phases will be telescoped or eliminated altogether, and there are also no doubt many cases in which decisions are made in a far more impulsive, informal, and haphazard manner. All of these processes will be determined in individual cases both by the nature of the group and its dynamics, above all the characteristics of its leaders and their style and method of making decisions, as well as by external factors such as changes in the security environment, the group's links with other actors whose assistance may be necessary, and a variety of other factors elucidated in our report. In short, in the "real world" there are many possible paths that may lead from ideological proclivities to operational objectives to final target selection, but these can only be determined with more specificity after in-depth qualitative studies of particular groups have been carried out. Our admittedly preliminary framework endeavors to take what is clearly a complex tangle of factor influences and shape them into something that is usable at once by analysts and security officials whose task it is to protect the U.S. homeland.

C. Limitations and Future Opportunities

Despite the study's significant findings, the project team has identified a number of areas that could benefit from further investigation and development. Such additional efforts would serve both to broaden and deepen our understanding of terrorist motivations for attacking CI, as well as refine the study in ways that would make it more accessible and useful to the policy, security, and research communities. Three aspects of the project, in particular, should be highlighted as areas that offer opportunities for valuable future development:

Case Studies. As has been demonstrated by the cases included in this report, qualitative case studies are uniquely well-suited to enhancing our understanding of the significant – but frequently difficult to observe and quantify – factors and dynamics that influence terrorist decision making. Unfortunately, the proper preparation of such case studies requires a considerable investment in time and/or manpower, and usually requires the involvement of researchers who possess some specialized knowledge about the particular terrorist groups being considered. Indeed, information collection is more often constrained by tight deadlines than by a lack of available source material, especially when work is being proposed on topics that have rarely been examined by scholars, such as this one. A more complete understanding of terrorist motivations for attacking critical infrastructure could undoubtedly be gleaned from additional research into instances in which "really existing" terrorist groups intentionally carried out such attacks. In order to do such research properly, it would be necessary to examine a much wider corpus of primary and secondary sources than is typically consulted, including 1) ideological treatises, brochures, and communiqués that have been published and disseminated by particular terrorist groups; 2) internal documents produced by those groups, such as bulletins, instructions, or the summaries of strategy sessions that have been recovered as a result of law enforcement or other research activities; 3) intelligence documents and judicial materials concerning the activities of these groups; and 4) interviews, where possible, with former members of the groups, above all their leaders. After carefully examining these types of source materials, it would be possible to provide far greater insight into the decision-making processes of terrorist groups, including in the context of CI targeting.

Database. CNS' CrITIC Database is likely the most robust database – and apparently the *only* open source database – that has been exclusively designed to collect information about terrorist attacks on critical infrastructure. Although reasonably comprehensive given the limitations of the sources from which it was compiled – the only ones presently available –CrITIC is still in its early stages of development and can be further improved in an effort to provide more accurate and informative data and analysis. CNS considers the CrITIC database to be a "work in progress," a necessary foundation upon which even more fruitful work can be built in the future. To this end, it would be useful to be able to carry out three additional tasks in the near term. First, in order to confirm the validity of CrITIC – and thus ensure its credibility – each case in the database should ideally be investigated further in order to confirm the details. (Such investigations were not possible given the scope and time constraints of the current project.) Second, it was apparent that sufficient data was not readily available for determining factors such as "Type of Attack," "Terrorist Group Type," or "Scale of Impact," even for many of the more recent incidents. As a direct consequence, hundreds of cases in the database had to be classified as "Uncertain" and excluded from more detailed analysis. Additional research would help resolve such ambiguities and enhance CrITIC's dataset significantly.

Third, it should be noted that the initial quantitative analysis of CrITIC's information was limited by data and resource constraints. With additional time, more advanced statistical techniques – including logit and probit models – could be used to assess the interplay and relative significance of each variable with greater accuracy. Because these statistics were drawn largely from *international* incidents of terrorist attacks on CI, the extent to which they reflect U.S. domestic trends is debatable. As has already been mentioned, moreover, it was beyond the scope of this study to compare trends in terrorism in general with the trends in attacking CI in particular. As a result, there is a danger that the conclusions drawn herein could be misinterpreted. For example, although the lethality of CI attacks grew dramatically in the 1990s, so too did the lethality of terrorist attacks in general. Moreover, the seemingly striking increase in the number of recent attacks on CI might not appear so dramatic if one is mindful of the dramatic increase in the overall number of terrorist attacks during that same period. As is clear from the media's coverage of recent insurgent activities in Iraq, attacks on critical infrastructure are becoming an increasingly prominent aspect of contemporary non-state violence. Presently, the CrITIC Database only includes incidents up through March 2004. An active, ongoing effort to catalogue new CI terrorism incidents would be especially worthwhile in an effort to determine whether the increasing publicity given to CI vulnerabilities is in fact influencing terrorist target selection.

Framework. The DECIDe Framework constitutes an important first step toward developing an analytical tool that can be reliably used to help discern terrorist motivations for attacking CI. Even so, much work remains to be done. At this stage, the framework remains both overly complex and too cumbersome to be used easily. While its present iteration may be sufficient for a theoretical investigation such as this, in which all background information is vital, the model is by no means "user-friendly" in its current form. We feel that an urgent next step is to convert the current framework into a more streamlined product, preferably one that is presented in an interactive computer-based format. Given that the theoretical underpinnings of the framework have already been established, its transition from paper to PC should be a fairly straightforward exercise. It is also notable that the framework still contains a number of hypotheses. Those hypotheses that were included are held with a high degree of confidence by the project team. Still, they deserve additional scientific investigation and validation to ensure that the framework is as reliable as possible. Additionally, the framework itself requires testing, validation, and iterative improvement. This would optimally involve cases relating to currently active terrorist groups, and would provide an opportunity for further interaction between the product's users and developers. Finally, a significant limitation of the DECIDe Framework is that it is a "single shot" model that only focuses on terrorist motivations for discreet attacks. An important prospect for further research is to extend the model so that it can be used to evaluate longer term terrorist "campaigns." Several layers of complexity are added when similar analytical approaches are adopted for cases involving multiple attacks, including the strategic anticipation of the actions of external actors and more variance in internal group factors. The project team already has thoughts on how multiple attack cases might be best addressed in terms of the evolution of the current project.

D. Final Thoughts

It has justly been noted that "[m]ost human beings formulate decisions based on past or perceived future patterns rather than through rational choices between alternatives."[579] In an endeavor such as this, where the ultimate goal is to gain predictive insight into the internal decision-making processes of terrorists, such words serve as a wise reminder that people, whether operating as individuals or as a part of larger groups, usually make decisions on the basis of various contextual, historically-contingent, implicit, and indeed "non-rational" factors rather than by carefully weighing costs and benefits via some formal logical process. It follows that statistics, models, and abstract frameworks will likely never be able to fully capture the complexity or the idiosyncrasies of the human mind. Such tools, however, can provide researchers and analysts with important way stations on the path towards a better grasp of how terrorists might approach difficult, multifaceted choices such as target selection.

For an area of terrorism study as vital as target selection, it is surprising that so little qualitative *or* quantitative research has been focused specifically on how terrorists make targeting decisions. We have attempted to fill this inexplicable gap in the literature, primarily by demonstrating the type of results that can be achieved through the simultaneous utilization of a number of parallel approaches in the examination of the problem of terrorist motivations for attacking CI. Hopefully we have at least succeeded in showing that there are useful ways to go about assessing this crucial motivational element of the terrorist threat, even though our preliminary framework requires further development. Moreover, once it has been developed further, we believe that similar approaches and frameworks will be applicable to several other areas of terrorist behavior analysis.

Thankfully, if one excludes the Oklahoma City bombing and the 9/11 attacks, no truly devastating terrorist attacks have yet been carried out against U.S. critical infrastructure. However, the frequent public discussion of existing infrastructural vulnerabilities by both government officials and journalists can only serve to focus the attention of would-be attackers on infrastructural targets, if not to induce them to launch actual attacks on them. Moreover, there is no doubt that once a series of successful attacks has been made on our homeland's CI, this will be bound to encourage further attacks of this type. In short, the threat to infrastructural targets is clearly growing, even if it might be an overstatement to describe it as omnipresent or imminent. If security officials and analysts hope to prepare for and cope effectively with such an eventuality, the most important preliminary task is to understand which groups are most likely to attack CI and what their objectives are likely to be for doing so. These questions can only be answered when the specific motivations of different types of terrorist groups are better understood, and it was this crucial task that our report has sought to advance.

---

[579] Gary Klein, *Sources of Power: How People Make Decisions* (Cambridge, MA: MIT, 1998).

Master Bibliography*

Zohar Abdoolcarim, "The Philippines' Terrorist Refuge," *Time [Asia]*, February 17, 2003.

Zachary Abuza, *Militant Islam in Southeast Asia: Crucible of Terror* (Boulder: Lynne Rienner, 2003).

Gary Ackerman, "Beyond Arson? A Threat Assessment of the Earth Liberation Front," *Terrorism and Political Violence*, Volume 15, Number 4 (Winter 2004).

Gary Ackerman, "Modifications to Rational Choice Models: Prospect Theory & Integrative Complexity," Unpublished working paper, 1999.

Mikhail A. Alexseev, *Without Warning: Threat Assessment, Intelligence, and Global Struggle* (New York: St.Martins Press, 1997).

"Ammonium Nitrate Explosion at AZF Toulouse," ility Engineering website, April 4, 2003.

Philip Anderson, "Threat-Vulnerability Integration: A Methodology for Risk Assessment," Center for Strategic and International Studies, Washington D.C.

David E. Apter and Nagayo Sawa, *Against the State: Politics and Social Protest in Japan* (Cambridge: Harvard University, 1984).

Paul Arrighi and Francis Pomponi, *Histoire de la Corse* (Paris: Presses Universitaires de France, 1978).

Norman R. Augustine, "Managing the Crisis You Tried to Prevent," *Harvard Business Review*, November- December 1995.

Jeffrey M. Bale, "Islamism," in Richard F. Pilch and Raymond Zilinskas, eds., *Encyclopedia of Bioterrorism Defense* (New York: Wiley, 2004), forthcoming.

Jeffrey M. Bale, "The Chechen Resistance and Radiological Terrorism," unpublished report, July 2003.

Jeffrey M. Bale, "Terrorism, Right-Wing," in Bernard A. Cook, ed., *Europe since 1945: An Encyclopedia* (New York: Garland, 2001) pp. 1238-40.

James David Ballard, "A Preliminary Study of Sabotage and Terrorism as Transportation Risk Factors Associated With the Proposed Yucca Mountain High-Level Nuclear Facility," July 1998. Accessed on 04/27/2004 at: http://www.state.nv.us/nucwaste/trans/jballard.htm

Albert-László Barabási, *Linked: The New Science of Networks* (Cambridge: Perseus Publishing, 2002).

* This bibliography was prepared by Andrew Jayne.

Joseph A. Barbera, MD, Anthony G. Macintyre, MD and Craig A. DeAtley, PA-C, "Ambulances to Nowhere: American Critical Shortfall in Medical Preparedness for Catastrophic Terrorism," Belfer Center for Science and International Affairs, Discussion Paper 2001-15, Accessed on 03/11/2004 at: http://www.homelandsecurity.org/journal/articles/Ambulancesbarbera.htm

Richard K. Betts, "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable," *World Politics* 31, Princeton University Press, (October 1978), pp. 61-89.

Randy Borum, Robert Fein, BryanVossekuil, and John Berglund, "Threat Assessment: Defining an Approach for Evaluating Risk of Targeted Violence," *Behavioral Sciences and the Law* 17, (1999), pp. 323-337.

Terr F. Bott and Stephen Eisenhower, "Evaluating Complex Systems When Numerical Information is Sparse," Los Alamos National Laboratory.

Terry F. Bott, Stephen W. Eisenhower, Jonathan Kingson, and Brian P. Key, "A New Graphical Tool for Building Logic-Gate Trees," Los Alamos National Laboratory and Innovative Technical Solutions, Inc.

William J. Broad, "Experts Call for Better Assessment of Threats," *New York Times (on the web)*, October 2, 2001. Accessed 10/2/2001.

Rob Buschmann, "Risk Assessment in the Presidents National Strategy for Homeland Security," Congressional Research Service Report for Congress, October 31, 2002.

Gavin Cameron, *Nuclear Terrorism: A Threat Assessment for the 21st Century* (New York: St. Martin's Press, 1999).

Peter Chalk, "Al-Qaeda and its Links to Terrorist Groups in Asia," in Andrew Tan and Kumar Ramakrishna, eds., *The New Terrorism: Anatomy, Trends and Counter-Strategies* (Singapore: Eastern Universities Press, 2002).

Peter Chalk, "Militant Islamic Extremism in the Southern Philippines," in Jason F. Isaacson and Colin Rubenstein, eds., *Islam in Asia: Changing Political Realities* (New Brunswick: Transaction, 2002).

Chukaku-ha website, which can be found at: www.zenshin.org/english_home/nc_intro.htm.

Codex Alimentarius Commission, "Principles and Guidelines for the Conduct of Microbiological Risk Assessment," CAC/GL-30, 1999.

Michael Corcoran, *Threat Assessment and Violence Intervention: A Practitioner's Handbook* (Boca Raton: CRC Press, 2003).

Xavier Crettiez, *La question corse* (Paris: Complexe, 1999).

Paul K. Davis, James H. Bigelow, and Jimmie McEver, "Exploratory Analysis and a Case History of Multiresolution, Multiperspective Modeling," Reprinted from Proceedings of the 2002 Winter Simulation Conference, Jeffrey A. Joines, Russell R. Barton, K. Kang, and Paul A. Fishwick (editors), December 2000 and Proceedings of the SPIE, Vol.4026, 2000.

Robert F. Dacey, "Critical Infrastructure Protection: Challenges in Securing Control Systems," Information Security Issues, Testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, House Committee on Government Reform, October 1, 2003.

Department of Defense Critical Infrastructure Protection (CIP) Plan, A Plan in Response to Presidential Decision Directive 63 "Critical Infrastructure Protection," Prepared by DASD (Security and Information Operations) Critical Infrastructure Protection Directorate, November 18, 1998.

Department of Defense, *DoD Responses to Transnational Threats,* The Defense Science Board 1997 Summer Study Task Force, Volume 1, Final Report, (Office of the Under Secretary of Defense for Acquisition and Technology, Washington, DC) October 1997.

Department of Energy, "Energy Infrastructure Vulnerability and Risk Assessment Checklists for State Governments," December 4, 2001. http://www.appanet.org/operations/checklist.pdf

Department of Homeland Security, Office for Domestic Preparedness, "State Homeland Security Assessment and Strategy Program."
http://www.shsasresources.com/documents/state_handbook.pdf

Department of Justice, "Assessment of the Increased Risk of Terrorist or Other Criminal Activity Associated with Posting Off-Site Consequence Analysis Information on the Internet," April 18, 2000.

Joseph DeRivera, Chapter 2: "The Construction of Reality," and Chapter 3: "The Projection of the Future," James N. Rosenau, consultant, *The Psychological Dimension of Foreign Policy* (Columbus, OH: C.E. Merrill Publishing Company, 1968), pp. 19-104.

Christopher Dobson and Ronal Payne, *The Weapons of Terror* (London: McMillan, 1979).

Sunil Donald, Terry F. Bott, and Stephen W. Eisenhower, "Representing Subjective Knowledge in Engineering Systems using Possibility Trees," Los Alamos National Laboratory, (July 2004).

C.J.M Drake, *Terrorists' Target Selection* (New York: St. Marten's Press, Inc, 1998).

DTRA, Cooperative Threat Reduction (CTR) Guide for Conducting Vulnerability Assessments.

S.W. Eisenhower, T. F. Bott, M.R. Sorokach, F. P. Jones, and J. R. Foggia, "Risk-Based Prioritization of Research for Aviation Security Using Logic-Evolved Decision Analysis," Los Alamos National Laboratory.

Steve Eisenhower, Terry Bott, and D.V. Rao, "Assessing the Risk of Nuclear Terrorism Using Logic Evolved Decision Analysis," Los Alamos National Laboratory (LA-UR-03-3467).

EPIC's Testimony to the House Subcommittee on Oversight and Investigations on "Creating the Department of Homeland Security: Consideration of the Administration's Proposal," July 9, 2002.

EPIC's Testimony to the Senate Committee on Governmental Affairs on "Securing Our Infrastructure: Private/Public Information Sharing," May 8, 2002.

EPIC's Letter to the House Judiciary Committee, Subcommittee on Crime, on H.R. 3482, The Cyber Security Enhancement Act of 2002, February 26, 2002.

EPIC's Testimony to the House Government Reform Committee on H.R. 4246, The Cyber Security Information Act, June 22, 2000.

EPIC's Testimony to the Senate Judiciary Committee on "Cyber Attack: The National Protection Plan and its Privacy Implications," February 1, 2000.

EPIC Press Release on "National Plan for Information Systems Protection," February 1, 2000.

Executive Order 13010-Critical Infrastructure Protection, Federal Register, Vol. 6, No. 138, July 17, 1996.

Executive Summary of "National Plan for Information Systems Protection", January 7, 2000.

Jonathan David Farley, "Breaking Al Qaeda Cells: A Mathematical Analysis of Counterterrorism Operations (A Guide for Risk Assessment and Decision Making), *Studies in Conflict & Terrorism* 26, (2003), pp. 399–411.

Gilles Fauconnier and Mark Turner, *The Way We Think* (New York: Basic Books, 2002).

Federal Emergency Management Agency (FEMA), *Understanding Your Risks: Identifying Hazards and Estimating Losses*, State and Local Mitigation Planning Guide, August 2001.

Robert A. Fein and Bryan Vossekuil. *Protective Intelligence and Threat Assessment Investigations: A Guide for State and Local Law Enforcement Officials*, U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, (Washington, DC) July 1998.

Robert A. Fein, Bryan Vossekuil, and Gwen A. Holden, "Threat assessment: An Approach to Prevent Targeted Violence," U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, July 1995.

Joe Fiorill, "U.S. Terrorism Commision Pushes Risk Assessment as Key to Spending," *Global Security Newswire*, Monday, December 15, 2003.

Baruch Fischhoff, Roxana M. Gonzalez, Deborah A. Small, and Jennifer S. Lerner, "Judged Terror Risk and Proximity to the World Trade Center," *Journal of Risk and Uncertainty* 26:2/3, (2003) pp. 137-151.

General Accounting Office, "Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors," Report to the Committee on Energy and Commerce, U.S. House of Representatives, February 2003.

T. J. S. George, *Revolt in Mindanao: The Rise of Islam in Philippine Politics* (Kuala Lumpur: Oxford University, 1980).

Peter Gordon Gowing, *Muslim Filipinos – Heritage and Horizon* (Quezon City: New Day, 1973).

Antoine-Marie Graziani, *Pascal Paoli: Père de la patrie corse* (Paris: Tallandier, 2002).

Rohan Gunaratna, *Inside Al Qaeda: Global Network of Terror* (New York: Columbia University Press, 2002).

Karen Guttieri, Michael D. Wallace, Peter Suedfeld, University of British Columbia, "The Integrative Complexity of American Decision Makers in the Cuban Missile Crisis," *Journal of Conflict Resolution* 39, No. 4, (Beverly Hills: Sage Publications, Inc., 1995).

H.R. 3162-130 (P.L. 107-56), Section 1016, as found at: http://www.epic.org/privacy/terrorism/hr3162.html

Chris Hawley, Gregory G. Noll, and Michael S. Hildebrand, "Operations Security for Public Safety Agencies: Special Operations for Terrorism and Hazmat Crimes," Interagency Operations Security (OPSEC) Support Staff, Operations Security, Monograph Series.

Bruce Hoffman, "Al Qaeda, Trends in Terrorism and Future Potentialities: An Assessment," *Studies in Conflict and Terrorism* 26 (November-December 2003), pp. 429-442.

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

Bruce Hoffman, "Terrorist Targeting: Tactics, Trends, and Potentialities," RAND, Santa Monica, California, 1992.

Bruce Hoffman, "The Modern Terrorist Mindset: Tactics, Targets, and Technologies," Center for the Study of Terrorism and Political Violence St. Andrews University, Scotland, October 1997. http://www.ciaonet.org/wps/hob03/

Ole R. Holsti, "Crisis Decision Making: Perspective from Four Levels of Analysis," *Behavior, Society and Nuclear War* 1, Philip E. Tetlock, et. al, ed., (New York: Oxford University Press, 1989).

Bruce K. Hope, "A Risk Assessment Perspective on Bioterrorist Threats to the U.S. Food Supply," unpublished paper.

Bruce K. Hope, "Using Fault Tree Analysis to Assess Bioterrorist Risks to the U.S. Food Supply," Oregon Department of Environmental Quality, Land Quality Division.

David Patrick Houghton, "The Role of Analogical Reasoning in Novel Foreign-Policy Situations," *British Journal of Political Science 26*, (October 1996).

Jeffrey Hunker, CIAO, memo to CICG Members regarding "Offsite Materials." Obtained by EPIC under the Freedom of Information Act.

International Association of Chiefs of Police, Section 3: Threat Assessment, http://www.theiacp.org/pubinfo/pubs/pslc/svthreat.htm

Brian A. Jackson, "Technology Acquisition by Terrorist Groups: Threat Assessment Informed by Lessons from Private Sector Technology Adoption," *Studies in Conflict and Terrorism* 24, (2001) pp. 183-213.

"Jaish-e-Mohammad Mujahideen E-Tanzeem," South Asia Terrorism Portal, http://www.satp.org

Irving L. Janis and Leon Mann, Chapter 3: "A Conflict Model of Decision Making," and Chapter 4: "Defective Search and Appraisal under High Conflict, *Decision Making: A Psychological Analysis of Conflict, Choice, and Commitment*, (New York: The Free Press, 1977), pp. 45-133.

Brian Jenkins, "Defense Against Terrorism," *Political Science Quarterly* 101, Reflections on Providing for "The common Good," (1986), pp. 773-786.

Robert Jervis, "Perceiving and Coping with Threat," *Psychology and Deterrence* (Baltimore, MD: Johns Hopkins University Press, 1989).

Robert Jervis, *Perception and Misperception in International Politics* (Princeton, NJ: Princeton University Press, 1976).

Salah Jubair, *Bangsamoro: A Nation Under Endless Tyranny* (Kuala Lumpur: IQ Marin, 1999).

Peter J. Katzenstein and Yutaka Tsujinaka, *Defending the Japanese State: Structures, Norms and the Political Responses to Terrorism and Violent Social Protest in the 1970s and 1980s*, (Ithaca, NY: Cornell University, 1991).

Ralph L. Keeney and Howard Raiffa, *Decisions with Multiple Objectives: Preferences and Value Tradeoffs* (Cambridge: Cambridge University Press, 1993).

Gilles Kepel, *The Revenge of God: The Resurgence of Islam, Christianity and Judaism in the Modern World* (University Park: Pennsylvania State University, 1994).

Patricia King, "'Vipers' in the 'Burbs," *Newsweek*, July 15, 1996.

Glenn Koller, *Risk Modeling for Determining Value and Decision Making* (Boca Raton, FL: Chapman & Hall/CRC, 2000).

C. F. Kurtz and D. J. Snowden, "The New Dynamics of Strategy: Sense-making in a Complex and Complicated World," *IBM Systems Journal* 42, Number 3, (2003), accessed online on July 27, 2004 at http://www.findarticles.com/p/articles/mi_m0ISJ/is_3_42/ai_108049867.

Ronald D. Lee, Associate Deputy Attorney General, Department of Justice, memo to Jeffrey Hunker, Director, Critical Infrastructure Assurance Office regarding the National Information Systems Protection Plan, March 8, 1999. Obtained by EPIC under the Freedom of Information Act.

Jack S. Levy, "Prospect Theory, Rational Choice, and International Relations" *International Studies Quarterly* 41, (March 1997), pp. 87-112.

Mark Irving Lichbach, *The Rebel's Dilemma* (Ann Arbor: University of Michigan Press, 1998), pp. ix-xiv, 50-99, and 167-77.

Matthew J. Littleton, "Information Age Terrorism: Toward Cyberterror," Navel Postgraduate School, Monterey, CA, December 1995, as found at: http://www.fas.org/irp/threat/cyber/docs/npgs/terror.htm

Andrew Macdonald, *The Turner Diaries: A Novel* (Hillsboro, WV: National Vanguard, 1999 [1980]), passim.

Cesar Adib Majul, *The Contemporary Muslim Movement in the Philippines* (Berkeley: Mizan, 1985).

W. K. Che Man, *Muslim Separatism: The Moros of Southern Philippines and the Malays of Southern Thailand* (Singapore: Oxford University, 1990).

Naomi Mandel and Steven J. Heine, "Terror Management and Marketing: He Who Dies With the Most Toys Wins," Wharton School of Business, University of Pennsylvania.

Bianca Markram, "An insoluble problem?," *Reactions* 24, July 2002. www.reactionsnet.com

Harry F. Martz and Mark E. Johnson, "Risk Analysis of Terrorist Attacks," *Risk Analysis* 7, (1987).

Gordon H. McCormick, "Terrorist Decision Making," *Annual Reviews in Political Science* 6 (2003) pp. 473-507.

Thomas M. McKenna, *Muslim Rulers and Rebels: Everyday Politics and Armed Separatism in the Southern Philippines* (Berkeley: University of California, 1998).

Edward F. Mickolus, *Terrorism, 1988 – 1991: A Chronology of Events and a Selectively Annotated Bibliography*, Bibliographies and Indexes in Military Studies, Number 6 (Greenwood Press, 1993).

Edward F. Mickolus, Todd Sandler, Jean M. Murdock, *International Terrorism in the 1980's: A Chronology of Events*, Vol. 2, 1984 – 1987, First Edition, (Ames: Iowa State University Press, 1989).

Edward F. Mickolus, Todd Sandler, Jean M. Murdock, *International Terrorism in the 1980's: A Chronology of Events*, Vol. 1, 1980-1983, First Edition, (Ames: Iowa State University Press, 1989).

Edward F. Mickolus, *Transnational Terrorism: A Chronicle of Events*, 1968-1979, (London: ALDWYCH Press, 1980).

Edward F. Mickolus, "How Do We Know We're Winning the War Against Terrorists? Issues in Measurement," *Studies in Conflict and Terrorism* 25, (2002), pp. 151-160.

Militia Operation Plan American Viper (Del City, OK: United Sovereigns, no date).

Ian I. Mitroff, Murat C. Alpaslan, "Preparing for Evil," Harvard Business Review, April 2003.

John Monohan, et. al., *Rethinking Risk Assessment: The MacArthur Study of Mental Disorder and Violence* (Oxford: Oxford University Press, 2001).

John Moteff, "Critical Infrastructure: A Primer," Congressional Research Service, Received Through CRS Web, August 13, 1998.

John Moteff, "Critical Infrastructures: Background, Policy and Implementation," Congressional Research Service, Received Through CRS Web, February 4, 2002.

Harald Muller, "Terrorism, Proliferation: A European Threat Assessment," Institute for Security Studies, Chaillot Papers #58, March 2003.

Brigitte L. Nacos, "The Terrorist Calculus behind 9-11: A Model for Future Terrorism;" *Studies in Conflict and Terrorism* 26, (2003) pp. 1-16.

National Infrastructure Protection Center, "Risk Management: An Essential Guide to Protecting Critical Assets," November 2002. http://www.nipc.gov/publications/nipcpub/P-Risk%20Management.pdf

National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, February 2003.

Office for Domestic Preparedness (OPD), "Vulnerability Assessment Methodologies Report," U.S. Department of Homeland Security, Phase I Final Report, July 2003.

G.G. Onishchenko, "Bioterrorism as Threat to Biological Security: Assessment of Healthcare Institutions Preparedness to Counteract Bioterrorism," Moscow Vestnik Rossiyskoy Akdemii Meditsinskikh Nauk, No. 4, Document ID: CEP 20030729000394, Version Number: 1, April 4, 2003.

Arpad Palfy, "Weapons System Selection and Mass-Casualty Outcomes," *Terrorism and Political Violence* 15, No.2 (Summer 2003), pp. 81-95.

John Parachini, *Combating Terrorism: Assessing Threats, Risk Management, and Establishing Priorities*, Testimony before the House Subcommittee on National Security, Veterans Affairs, and International Relations, July 26, 2000. http://cns/pubs/reports/paraterror.htm

Eric Pianin, "Study Assesses Risk of Attack on Chemical Plant," *The Washington Post*, Mar 12, 2002, p. A.08.

Jerrold M. Post, Keven G. Ruby; and Eric D. Shaw, "The Radical Group in Context: An Integrated Framework for the Analysis of Group Risk for Terrorism," *Studies in Conflict and Terrorism* 25 (2002), p. 73-126.

President's Commission on Critical Infrastructure Protection, "Critical Foundations: Protecting America's Infrastructures," October 1997, as found at: http://www.dtra.mil/press_resources/publications/deskbook/full_text/Other_Relevant_References/PCCIP_Report.pdf

Marisa Reddy Pynchon and Randy Borum, "Assessing Threat of Targeted Group Violence: Contributions from Social Psychology," *Behavioral Sciences and the Law* 17 (1999), pp. 339-355.

[al-Qā`ida], *'I'alān al-Jihād 'ala al-Tawāghīt al-Bilād* (no publication information)

Chris Quillen, "A Historical Analysis of Mass Casualty Bombers," *Studies in Conflict and Terrorism* 25, (September-October 2002), pp. 279-292.

Kevin M. Quinley, Donald L. Schumidt, *Business at Risk; How to Assess, Mitigate, and respond to Terrorist Threats,* The National Underwriter Company, Cincinnati, Ohio, 2002.

Robert Ramsay, *The Corsican Time-Bomb* (Manchester: Manchester University, 1983).

"Remarks by the President to the Philippine Congress," full text on White House website, 18 October 2003. www.whitehouse.gov/news/releases/2003/10/print/20031018-12.html

Magnus Ranstorp, "Terrorism in the Name of Religion," in Russell D. Howard and Reid L. Sawyer eds., *Terrorism and Counterterrorism: Understanding the New Security Environment* (Guilford, CT: McGraw-Hill, 2002).

Simon Reeve, The New Jackals: Ramzi Yousef, Osama bin Ladin and the Future of Terrorism (Boston: Northeastern University, 1999).

Nancy A. Renfroe, and Joseph L. Smith, "Threat/Vulnerability Assessments and Risk Analysis," Whole Building Design Guide, Accessed on 03/11/2004 at: http://www/wbdg/org/design/res-print.php?rp=27

Report of the President's Commission on Critical Infrastructure Protection, "Protecting America's Infrastructures," October 1997.

Vladimir P. Reshetin and James L. Regens, "Simulation Modeling of Anthrax Spore Dispersion in a Bioterrorism Incident," *Risk Analysis* 23, December 1, 2003.

Maria A. Ressa, *Seeds of Terror: An Eyewitness Account of Al-Qaeda's Newest Center of Operations in Southeast Asia* (New York: Free Press, 2003).

Colin Robson, *Real World Research: A Resource for Social Scientists and Practitioner-Researchers* (Oxford: Blackwell Publishers, 1993).

Jean-Michel Rossi and François Santoni, *Pour solde de tout compte: Les nationalistes corses parlent* (Paris: Denoël, 2000).

Barry Rubin, ed., *Revolutionaries and Reformers: Contemporary Islamist Movements in the Middle East* (Albany, NY: State University of New York, 2003).

Todd Sandler and Daniel G. Arce M., "Terrorism & Game Theory," *Simulation and Gaming* 34, (September 2003), pp. 319-337.

Jean-Pierre Santini, *Front de Libération Nationale de la Corse: De l'ombre à la lumière* (Paris: L'Harmattan, 2000).

Linda-Jo Schierow, "Chemical Plant Security," Report for Congress, Congressional Research Service, Received Through CRS Web, Updated January 23, 2003.

Linda-Jo Schierow, "The Role of Risk Analysis and Risk Management in Environmental Protection," Congressional Research Service Issue Brief for Congress, September 4, 2003.

Alex P. Schmid and Albert J. Jongman, *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories and Literature* (Amsterdam: North-Holland, 1988).

Bruce Schneier, *Secrets and Lies: Digital Security in the Networked World* (Wiley Publishing, Inc., 2004).

Elaine Shannon, "Learning from Terror Alerts," *Time*, July 14, 2004.

Andrew Silke, "Beating the Water: The Terrorist Search for Power, Control, and Authority," *Frank Cass Journals Terrorism and Political Violence* 12, (Summer 2000), pp. 76-96.

Edmond Simeoni, *Le piège d'Aléria:Les raisons de la colère des Corses* (Paris: J. C. Lattès, 1976).

Joshua Sinai, "Analytical Model of Terrorism Forecasting," paper, International Conference on Post Modern Terrorism, September 2003.
http://cnsinfo.miis.edu/search97cgi/s97_cgi?action...l&queryzip=%22threat+assessment%22&Collection=FBIS

Joshua Sinai, "ICT Conference: Expert on Value, Methods of Forecasting Terrorist Incidents," FBIS Report, Document ID: GMG20031202000085, September 9, 2003.

Captain Robert L. Snow, *The Militia Threat: Terrorists Among Us* (New York and London: Plenum Trade, 1999).

Anthony Spaeth, "First Bali, now Davao," *Time [Asia]*, March 10, 2003.

Paul C. Stern and Harvey V. Fineberg. Eds. *Understanding Risk: Informing Decisions in a Democratic Society* (Washington D.C.: National Academy Press, 1996).

Peter St. John, *Air Piracy, Airport Security, and International Terrorism: Winning the War against Hijackers* (New York: Quorum Books, 1991), pp. 5, 43-66, Appendices 2, 3, and 7.

Cass R. Sunstein, "Terrorism and Probability Neglect," *Journal of Risk and Uncertainty* 26:2/3; (2003) pp. 137-151.

Nassim Nicholas Taleb, "The Black Swan: Why Don't We Lean that We Don't Learn?," Highland Forum 23, Las Vegas, November 2003, First Draft, January 2004.

Bron Taylor, "Religion, Violence, and Environmentalism," *Terrorism and Political Violence*, Vol. 10, #4, Winter 1998. http://www.religionandnature.com/bron/TPV%20article.htm.

"Terror from the Right," *SPLC Intelligence Report* 102 (Summer 2001).

The American Heritage Dictionary of the English Language, William Morris, (editor), New College Edition, (Boston: Houghton Mifflin Co., 1981).

Troy S. Thomas, Maj., USAF and William D. Casebeer, Maj., USAF, "Violent Non-State Actors: Countering Dynamic Systems," *Strategic Insights* 3, (March 2004).

U.S. Department of Homeland Security: Office for Domestic Preparedness (OPD), "Vulnerability Assessment Methodologies Report," Phase I Final Report, July 2003.

U.S. Department of Homeland security, FEMA, "Risk Management Series, Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings," December 2003.

U.S. Department of State, *1996 Patterns of Global Terrorism* (Washington, DC: Government Printing Office, 1997), as found at:
http://www.state.gov/www/global/terrorism/annual_reports.html

U.S. General Accounting Office, "Homeland Security: Voluntary Initiatives Are Under Way at Chemical Facilities, but the Extent of Security Preparedness is Unknown," March 2003.

U.S. General Accounting Office, "Combating Terrorism: Actions Needed to Guide Services' Antiterrorism Efforts at Installations," November 2002.

U.S. General Accounting Office, "Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism," February 2004.

U.S. General Accounting Office, "Combating Terrorism: Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attacks," September 1999.

U.S. General Accounting Office. "Combating Terrorism: Threat And Risk Assessments Can Help Prioritize and Target Program Investments". GAO/NSIAD-98-74.

U.S. General Accounting Office, "Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors," Report to the Committee on Energy and Commerce, House of Representatives, February 2003.

U.S. General Accounting Office, "Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities," Report to the Subcommittee on Technology, Terrorism, and Government Information, Committee on the Judiciary, U.S. Senate, April 2001.

U.S. General Accounting Office, "Transportation Security Research: Coordination Needed in Selecting and Implementing Infrastructure Vulnerability Assessments," May 2003.

U.S. House of Representatives, Committee on Government Reform, Subcommittee on National Security, Veterans Affairs, and International Relations, "Hearing on Combating Terrorism: Assessing Threats, Risk Management and Establishing Priorities," One Hundred Sixth Congress, Second Session, July 26, 2000, Serial No. 106-253. http://www.gpo.gov/congress/house or http://www.house.gov/reform

U.S. District Court, District of Colorado, *United States of America v. Timothy James McVeigh and Terry Lynn Nichols*.

U.S. District Court, Southern District, *Unites States of America v. Omar Ahmad Ali Abdel Rahman*.

U.S. General Accounting Office, Report to Congressional Requesters, *Combating Terrorism: Threat And Risk Assessments Can Help Prioritize and Target Program Investments*, (Washington, DC, National Security and International Affairs Division, April 1998) GAO/NSIAD-98-74

Ben Venzke and Aimee Ibrahim, *The al-Qaeda Threat: An Analytical Guide to al-Qaeda's Tactics and Targets* (Alexandria, VA: Tempest, 2003).

W. Kip Viscusi and Richard J. Zeckhauser, "Sacrificing Civil Liberties to Reduce Terrorism Risks," *Journal of Risk and Uncertainty* 26, March-May 2003.

Marites Dañguilan Vitug and Glenda M. Gloria, *Under the Crescent Moon: Rebellion in Mindanao,* (Quezon City: Ateneo Center for Social Policy and Public Affairs/Institute for Popular Democracy, 2000).

Michael D. Watkins, Max H. Bazerman, "Predictable Surprises: Disasters You Should Have Seen Coming," *Harvard Business Review*, March 2003.

Robert W. White, "Issues in the Study of Political Violence: Understanding the Motives of Participants in Small Group Political Violence," *Terrorism and Political Violence* 12, (Spring 2000), pp. 95-108.

Transcript of White House Press Briefing on "Cyber-Security," January 7, 2000.

White House, "Defending America's Cyberspace: National Plan for Information Systems Protection, Version 1.0," 2000.

White House, "Executive Order 13010 – Critical Infrastructure Protection," July 15, 1996, as found at: http://www.fas.org/irp/offdocs/eo13010.htm

White House, "Executive Order 13228 – Establishing the Office of Homeland Security and the Homeland Security Council," October8, 2001, as found at: http://www.whitehouse.gov/news/releases/2001/10/20011008-2.html.

White House, "Executive Order 13231 – Critical Infrastructure Protection in the Information Age," October 16, 2001, as found at: http://www.fas.org/irp/offdocs/eo/eo-13231.htm.

White House, "Homeland Security Presidential Directive 7 – Critical Infrastructure Identification, Prioritization, and Protection," December 17, 2003, as found at: http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html

White House "National Plan for Information Systems Protection", January 7, 2000.

White House, "National Strategy for Homeland Security," July 16, 2002, as found at: http://www.whitehouse.gov/homeland/book/sect3-3.pdf

White House, "Presidential Decision Directive/NSC-63 – Critical Infrastructure Protection," May 22, 1998, as found at: http://www.fas.org/irp/offdocs/pdd/pdd-63.htm

White House Press Release on "Cyber-Security", January 7, 2000.

Rick Whiting, "Companies Boost Sales Efforts with Predictive Analysis," Information Week, Accessed on 6/7/2002. http://www.informationweek.com/story/IWK20020221s0018

Dr. Gordon Woo, "The al-Qaeda War Game: Following the Path of Least Resistance," Risk Management Solutions. http://www.rms.com/Publications/AlQaedaWarGame_Woo.asp

Dr. Gordon Woo, "The evolution of Terrorism Risk Modeling," Risk Management Solutions. http://www.rms.com/Publications/EvolutionTerRiskMod_Woo_JournalRe.pdf

Dr. Gordon Woo, "Mathematical Aspects of Terrorism Hazard", Risk Management Solutions. http://www.rms.com/Publications/MathematicalAspectsOfTerrorHaz_Woo.asp

Dr. Gordon Woo, "Quantitative Terrorism Risk Assessment," Risk Management Solutions, http://www.rms.com/NewsPress/Quantitative_Terrorism_Risk_Assessment.pdf

Dr. Gordon Woo, "Understanding Terrorism Risk," Risk Management Solutions, http://www.rms.com/Publications/UnderstandTerRisk_Woo_RiskReport04.pdf

Don Wynegar, Communications and Information Infrastructure Assurance Program (CIIAP) FY 2000, Presentation to Communications and Information Sector Working Group, May 30, 2000. (PowerPoint presentation)

Raymond A. Zilinskas, "Bioterrorism Threat Assessment and Risk Managements Workshop," Final Report and Commentary from bioterrorism threat assessment and risk management workshop November 12-13, 2001, Washington D.C. office of Center For Nonproliferation Studies, Monterey Institute of International Studies, June 24, 2003.

Raymond A. Zilinskas, "Bioterrorism Threat Assessment and Risk Managements Workshop: Final Report and Commentary," Presented to the U.S. Department of Energy, Monterey Institute of International Studies, No. 17, June 24, 2003.

Case Study Bibliography*

Zohar Abdoolcarim, "The Philippines' Terrorist Refuge," *Time [Asia]*, 17 February 2003

Zachary Abuza, *Militant Islam in Southeast Asia: Crucible of Terror* (Boulder: Lynne Rienner, 2003).

David E. Apter and Nagayo Sawa, *Against the State: Politics and Social Protest in Japan,* (Cambridge: Harvard University, 1984).

"Ammonium Nitrate Explosion at AZF Toulouse," ility Engineering website, 4 April 2003.

Paul Arrighi and Francis Pomponi, *Histoire de la Corse* (Paris: Presses Universitaires de France, 1978).

Jeffrey M. Bale, "Islamism," in Richard F. Pilch and Raymond Zilinskas, eds., *Encyclopedia of Bioterrorism Defense* (New York: Wiley, 2004), forthcoming.

Jeffrey M. Bale, "The Chechen Resistance and Radiological Terrorism," unpublished report, July 2003.

Jeffrey M. Bale, "Terrorism, Right-Wing," in Bernard A. Cook, ed., *Europe since 1945: An Encyclopedia* (New York: Garland, 2001) pp. 1238-40.

Peter Chalk, "Al-Qaeda and its Links to Terrorist Groups in Asia," in Andrew Tan and Kumar Ramakrishna, eds., *The New Terrorism: Anatomy, Trends and Counter-Strategies*, (Singapore: Eastern Universities Press, 2002).

Peter Chalk, "Militant Islamic Extremism in the Southern Philippines," in Jason F. Isaacson and Colin Rubenstein, eds., *Islam in Asia: Changing Political Realities* (New Brunswick: Transaction, 2002).

Chukaku-ha website, which can be found at: www.zenshin.org/english_home/nc_intro.htm.

Xavier Crettiez, *La question corse,* (Paris: Complexe, 1999).

T. J. S. George, *Revolt in Mindanao: The Rise of Islam in Philippine Politics* (Kuala Lumpur: Oxford University, 1980).

Peter Gordon Gowing, *Muslim Filipinos – Heritage and Horizon* (Quezon City: New Day, 1973).

Antoine-Marie Graziani, *Pascal Paoli: Père de la patrie corse* (Paris: Tallandier, 2002).

Rohan Gunaratna, *Inside Al Qaeda: Global Network of Terror* (New York: Berkley, 2002).

* This bibliography was prepared by Andrew Jayne.

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

Salah Jubair, *Bangsamoro: A Nation Under Endless Tyranny* (Kuala Lumpur: IQ Marin, 1999).

Peter J. Katzenstein and Yutaka Tsujinaka, *Defending the Japanese State: Structures, Norms and the Political Responses to Terrorism and Violent Social Protest in the 1970s and 1980s* (Ithaca, NY: Cornell University, 1991).

Gilles Kepel, *The Revenge of God: The Resurgence of Islam, Christianity and Judaism in the Modern World* (University Park: Pennsylvania State University, 1994).

Patricia King, "'Vipers' in the 'Burbs," *Newsweek*, 15 July 1996

Matthew J. Littleton, "Information Age Terrorism: Toward Cyberterror," Navel Postgraduate School, Monterey, CA, December 1995, as found at: http://www.fas.org/irp/threat/cyber/docs/npgs/terror.htm.

Andrew Macdonald (pseudonym for Pierce), *The Turner Diaries: A Novel* (Hillsboro, WV: National Vanguard, 1999 [1980]), passim.

Cesar Adib Majul, *The Contemporary Muslim Movement in the Philippines* (Berkeley: Mizan, 1985).

Thomas M. McKenna, *Muslim Rulers and Rebels: Everyday Politics and Armed Separatism in the Southern Philippines* (Berkeley: University of California, 1998).

W. K. Che Man, *Muslim Separatism: The Moros of Southern Philippines and the Malays of Southern Thailand* (Singapore: Oxford University, 1990).

Militia Operation Plan American Viper (Del City, OK: United Sovereigns, no date).

[al-Qā`ida], *'I'alān al-Jihād 'ala al-Tawāghīt al-Bilād* (no publication information)

Robert Ramsay, *The Corsican Time-Bomb* (Manchester: Manchester University, 1983).

Magnus Ranstorp, "Terrorism in the Name of Religion," in Russell D. Howard and Reid L. Sawyer eds., *Terrorism and Counterterrorism: Understanding the New Security Environment* (Guilford, CT: McGraw-Hill, 2002).

"Remarks by the President to the Philippine Congress," full text on White House website, 18 October 2003: www.whitehouse.gov/news/releases/2003/10/print/20031018-12.html

Simon Reeve, *The New Jackals: Ramzi Yousef, Osama bin Ladin and the Future of Terrorism* (Boston: Northeastern University, 1999).

Maria A. Ressa, *Seeds of Terror: An Eyewitness Account of Al-Qaeda's Newest Center of Operations in Southeast Asia* (New York: Free Press, 2003).

Jean-Michel Rossi and François Santoni, *Pour solde de tout compte: Les nationalistes corses parlent* (Paris: Denoël, 2000).
Barry Rubin, ed., *Revolutionaries and Reformers: Contemporary Islamist Movements in the Middle East* (Albany, NY: State University of New York, 2003).

Jean-Pierre Santini, *Front de Libération Nationale de la Corse: De l'ombre à la lumière* (Paris: L'Harmattan, 2000).

Alex P. Schmid and Albert J. Jongman, *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories and Literature* (Amsterdam: North-Holland, 1988).

Elaine Shannon, "Learning from Terror Alerts," *Time*, 14 July 2004.

Edmond Simeoni, *Le piège d'Aléria:Les raisons de la colère des Corses* (Paris: J. C. Lattès, 1976).

Captain Robert L. Snow, *The Militia Threat: Terrorists Among Us* (New York and London: Plenum Trade, 1999).

Anthony Spaeth, "First Bali, now Davao," *Time [Asia]*, 10 March 2003.

Bron Taylor, "Religion, Violence, and Environmentalism," *Terrorism and Political Violence*, Vol. 10, #4, Winter 1998. http://www.religionandnature.com/bron/TPV%20article.htm.

"Terror from the Right," *SPLC Intelligence Report* 102, (Summer 2001).

U.S. Department of State, *1996 Patterns of Global Terrorism* (Washington, DC: Government Printing Office, 1997), as found at:
http://www.state.gov/www/global/terrorism/annual_reports.html

United States District Court, District of Colorado, *United States of America v. Timothy James McVeigh and Terry Lynn Nichols*.

United States District Court, Southern District, *United States of America v. Omar Ahmad Ali Abdel Rahman*.

Ben Venzke and Aimee Ibrahim, *The al-Qaeda Threat: An Analytical Guide to al-Qaeda's Tactics and Targets* (Alexandria, VA: Tempest, 2003).

Marites Dañguilan Vitug and Glenda M. Gloria, *Under the Crescent Moon: Rebellion in Mindanao* (Quezon City: Ateneo Center for Social Policy and Public Affairs/Institute for Popular Democracy, 2000).

Critical Infrastructure Bibliography*

Robert F. Dacey, "Critical Infrastructure Protection: Challenges in Securing Control Systems," Information Security Issues, Testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, House Committee on Government Reform, October 1, 2003.

Department of Defense Critical Infrastructure Protection (CIP) Plan, A Plan in Response to Presidential Decision Directive 63 "Critical Infrastructure Protection," Prepared by DASD (Security and Information Operations) Critical Infrastructure Protection Directorate, November 18, 1998.

Department of Justice, Assessment of the Increased Risk of Terrorist or Other Criminal Activity Associated with Posting Off-Site Consequence Analysis Information on the Internet, April 18, 2000.

Executive Order 13010-Critical Infrastructure Protection, Federal Register, Vol. 6, No. 138, July 17, 1996.

EPIC's Testimony to the House Subcommittee on Oversight and Investigations on "Creating the Department of Homeland Security: Consideration of the Administration's Proposal," July 9, 2002.

EPIC's Testimony to the Senate Committee on Governmental Affairs on "Securing Our Infrastructure: Private/Public Information Sharing," May 8, 2002.

EPIC's Letter to the House Judiciary Committee, Subcommittee on Crime, on H.R. 3482, The Cyber Security Enhancement Act of 2002, February 26, 2002.

EPIC's Testimony to the House Government Reform Committee on H.R. 4246, The Cyber Security Information Act, June 22, 2000.

EPIC's Testimony to the Senate Judiciary Committee on "Cyber Attack: The National Protection Plan and its Privacy Implications," February 1, 2000.

EPIC Press Release on "National Plan for Information Systems Protection," February 1, 2000.

Executive Summary of "National Plan for Information Systems Protection," January 7, 2000.

Jeffrey Hunker, CIAO, memo to CICG Members regarding "Offsite Materials." Obtained by EPIC under the Freedom of Information Act.

Ronald D. Lee, Associate Deputy Attorney General, Department of Justice, memo to Jeffrey Hunker, Director, Critical Infrastructure Assurance Office regarding the National Information

* This bibliography was prepared by Andrew Jayne.

Systems Protection Plan, March 8, 1999. Obtained by EPIC under the Freedom of Information Act.

John Moteff, "Critical Infrastructure: A Primer," Congressional Research Service, Received Through CRS Web, August 13, 1998.

John Moteff, "Critical Infrastructures: Background, Policy and Implementation," Congressional Research Service, Received Through CRS Web, February 4, 2002.

National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, February 2003.

Report of the President's Commission on Critical Infrastructure Protection, "Protecting America's Infrastructures," October 1997.

Linda-Jo Schierow, "Chemical Plant Security," Report for Congress, Congressional Research Service, Received Through CRS Web, Updated January 23, 2003.

Transcript of White House Press Briefing on "Cyber-Security", January 7, 2000.

United States General Accounting Office, "Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors," Report to the Committee on Energy and Commerce, House of Representatives, February 2003.

United States General Accounting Office, "Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities," Report to the Subcommittee on Technology, Terrorism, and Government Information, Committee on the Judiciary, U.S. Senate, April 2001.

United States General Accounting Office, "Transportation Security Research: Coordination Needed in Selecting and Implementing Infrastructure Vulnerability Assessments," May 2003.

White House, "Defending America's Cyberspace: National Plan for Information Systems Protection, Version 1.0," 2000.

White House "National Plan for Information Systems Protection", January 7, 2000.

White House, Presidential Decision Directive (PDD)/ NSC 63: Critical Infrastructure Protection, May 22, 1998.

White House Press Release on "Cyber-Security", January 7, 2000.

Don Wynegar, Communications and Information Infrastructure Assurance Program (CIIAP) FY 2000, Presentation to Communications and Information Sector Working Group, May 30, 2000. (PowerPoint presentation)

CrITIC Database Bibliography

Christopher Dobson and Ronal Payne's, *The Weapons of Terror* (London: McMillan, 1979).

Edward F. Mickolus, *Terrorism, 1988 – 1991: A Chronology of Events and a Selectively Annotated Bibliography*, Bibliographies and Indexes in Military Studies, Number 6 (Greenwood Press, 1993).

Edward F. Mickolus, Todd Sandler, Jean M. Murdock, *International Terrorism in the 1980's: A Chronology of Events*, (Ames: Iowa State University Press, 1989). Vol. 2, 1984 – 1987. First Edition.

Edward F. Mickolus, Todd Sandler, Jean M. Murdock, *International Terrorism in the 1980's: A Chronology of Events*, (Ames: Iowa State University Press, 1989). Vol. 1, 1980-1983. First Edition.

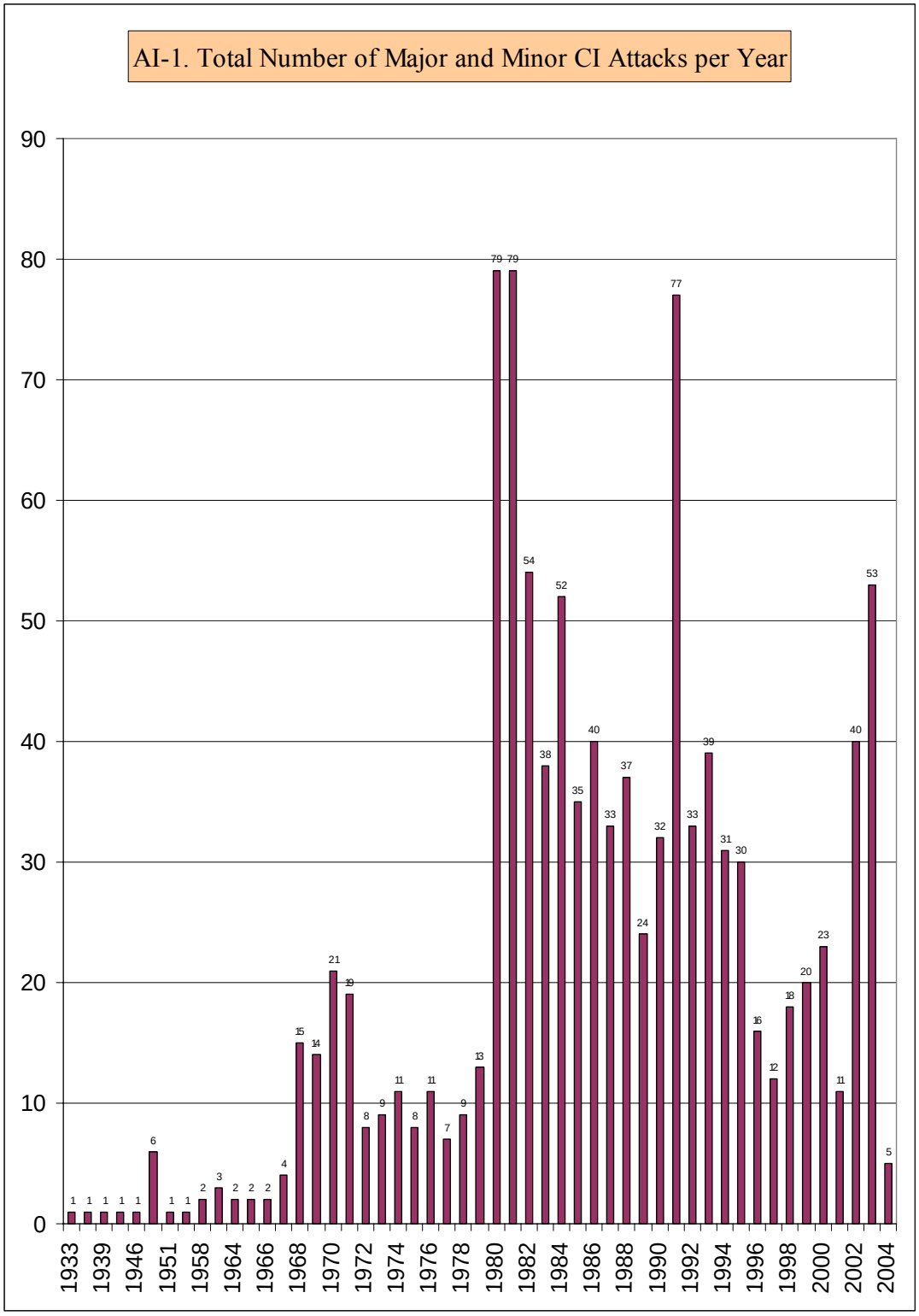
Edward F. Mickolus, *Transnational Terrorism: A Chronicle of Events*, 1968-1979, (London: ALDWYCH Press, 1980).

Colin Robson, *Real World Research: A Resource for Social Scientists and Practitioner-Researchers* (Oxford: Blackwell Publishers, 1993).

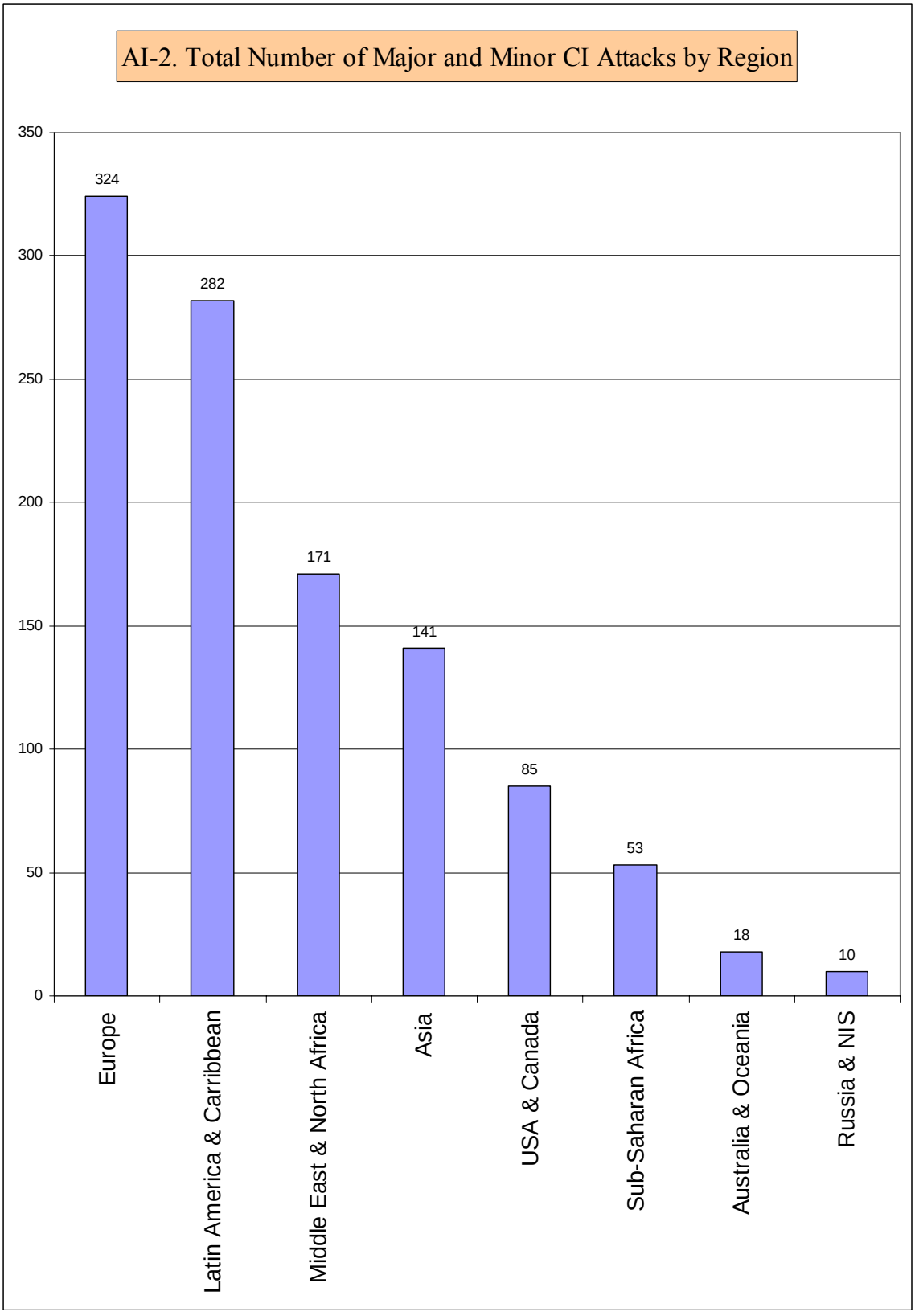
Dr. Joshua Sinai, "ICT Conference: Expert on Value, Methods of Forecasting Terrorist Incidents," FBIS Report, Document ID: GMG20031202000085, September 9, 2003.

Raymond A. Zilinskas, "Bioterrorism Threat Assessment and Risk Managements Workshop: Final Report and Commentary," Presented to the U.S. Department of Energy, Monterey Institute of International Studies, No. 17, June 24, 2003.

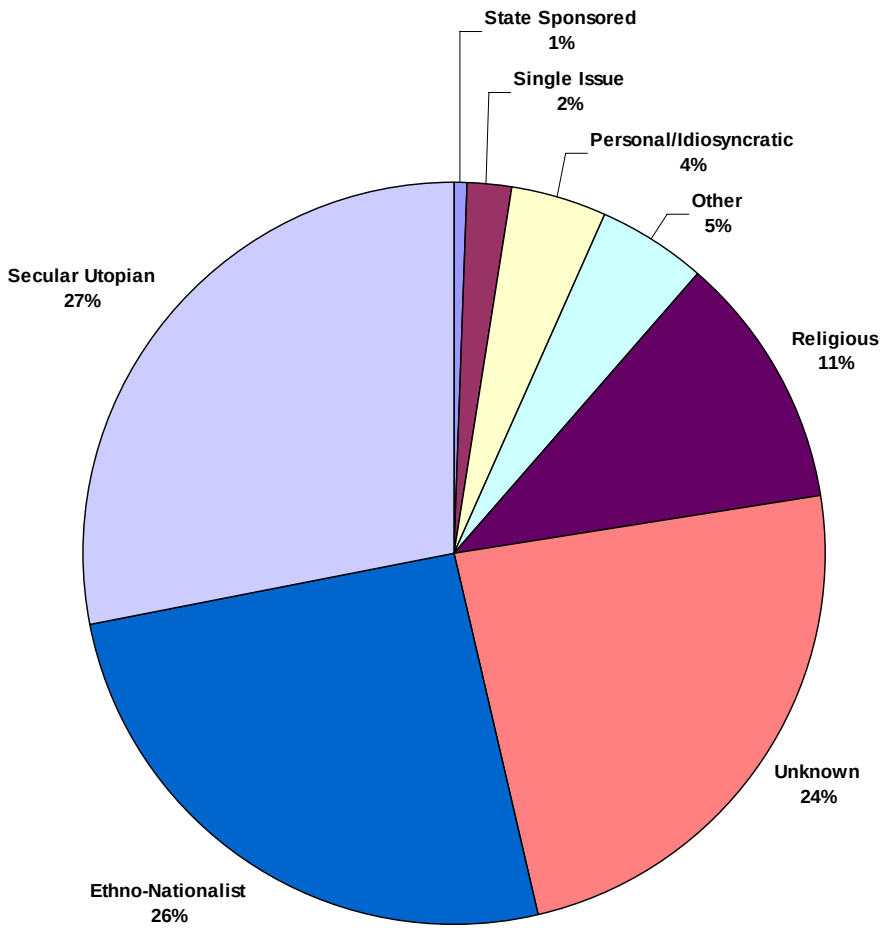
Appendix I: CHARTS DERIVED FROM CrITIC *



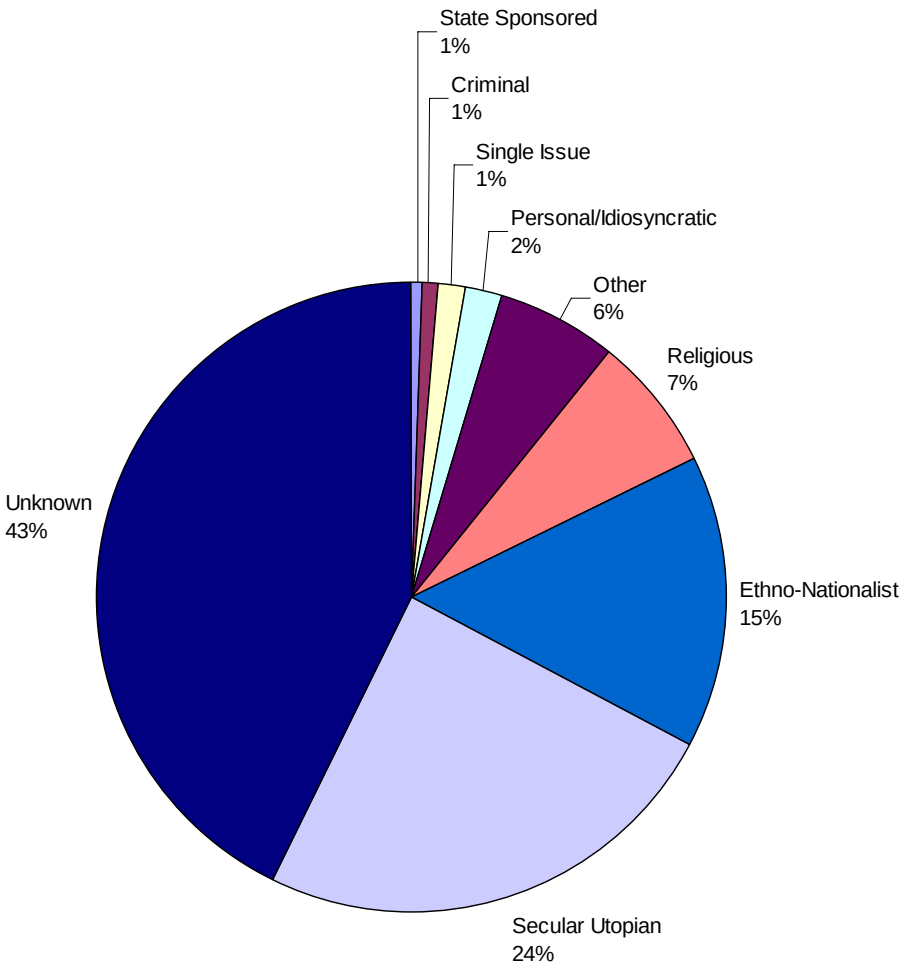
* This appendix was prepared by Praveen Abhayaratne, Charles Blair, and Sundara Vadlamudi.

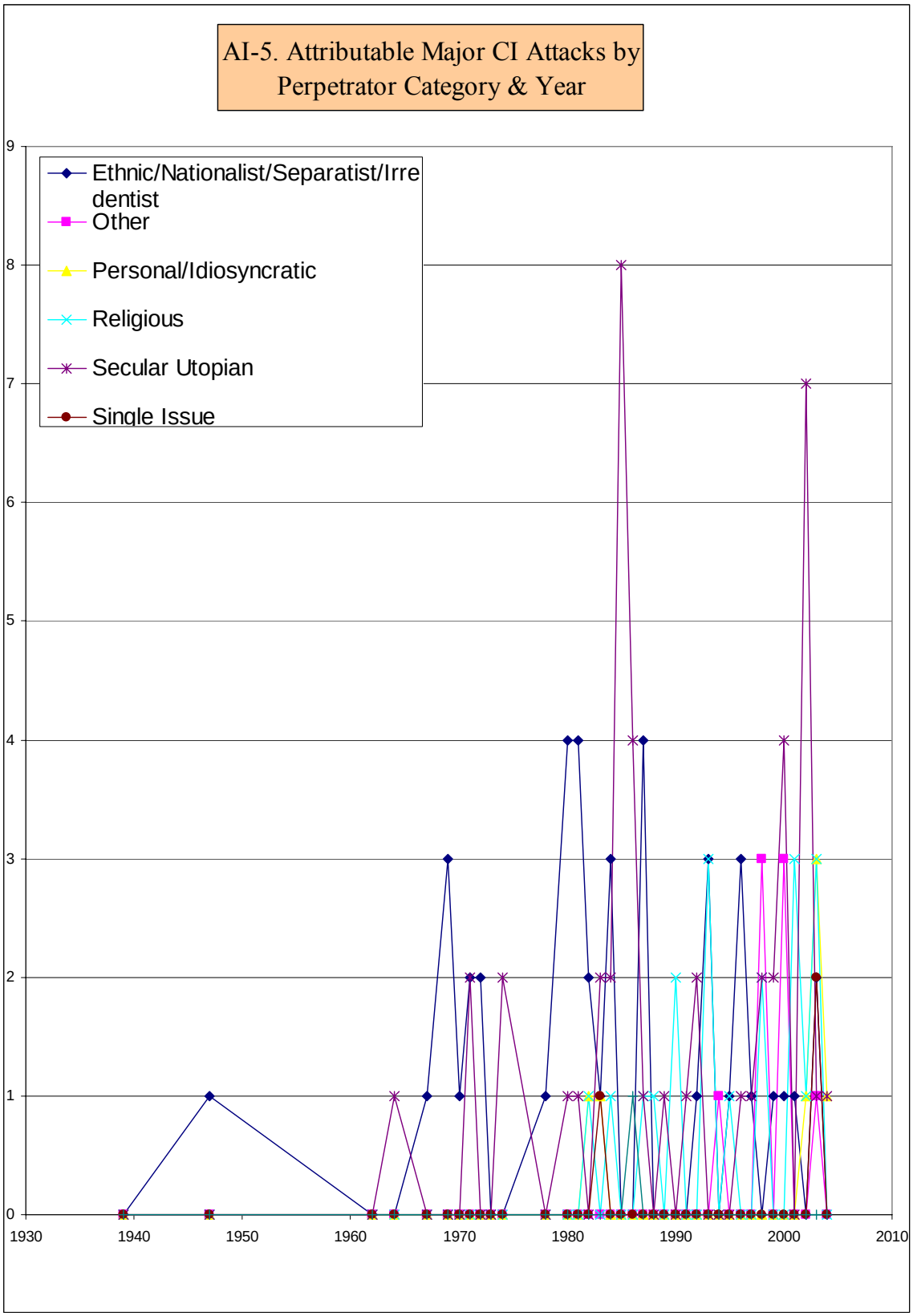

AI-2. Total Number of Major and Minor CI Attacks by Region
350
300
250
200
150
100
50
0
324
282
171
141
85
53
18
10
Europe
Latin America & Carribbean
Middle East & North Africa
Asia
USA & Canada
Sub-Saharan Africa
Australia & Oceania
Russia & NIS

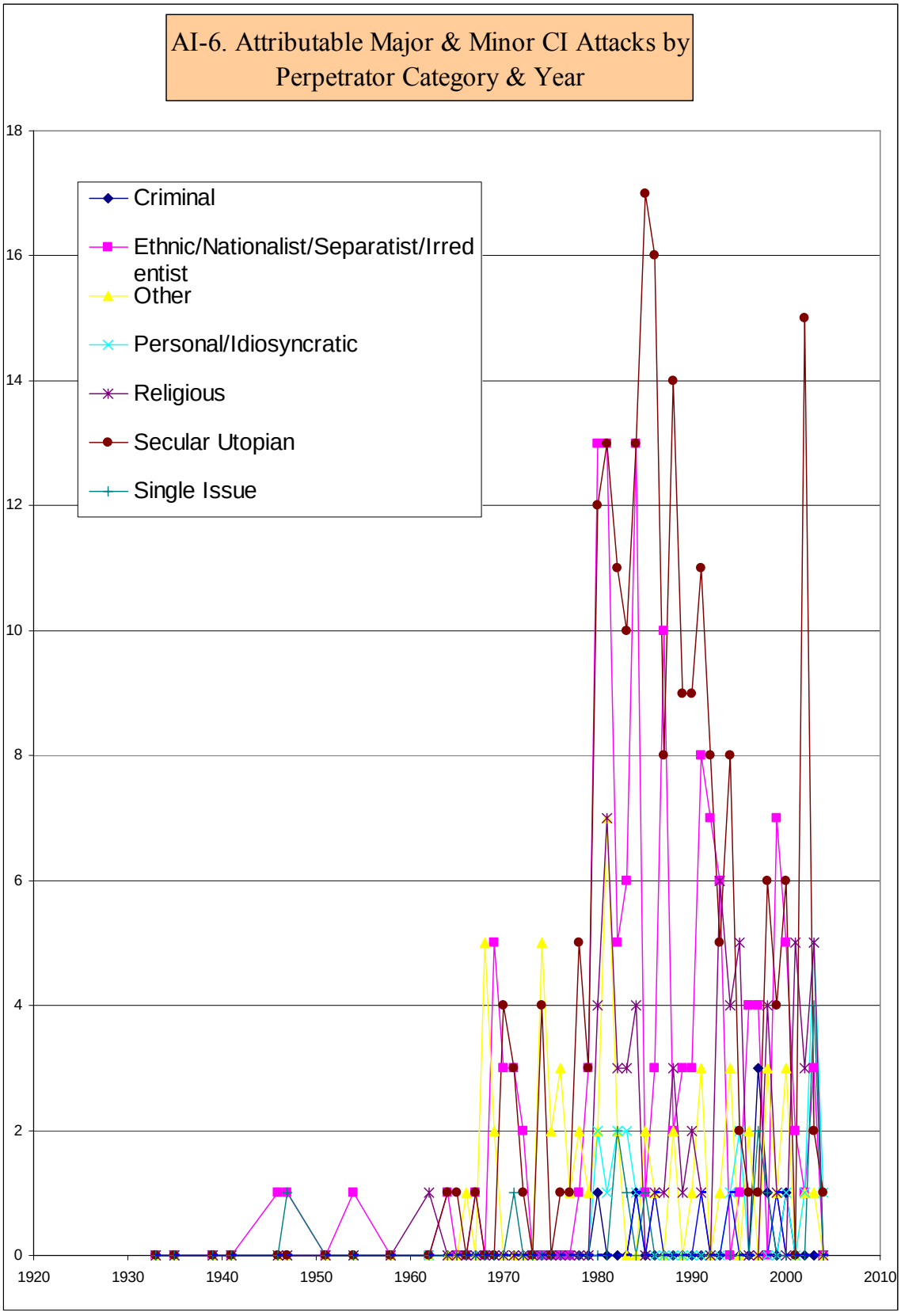
AI-3. Attributable Major CI Attacks by Perpetrator Category



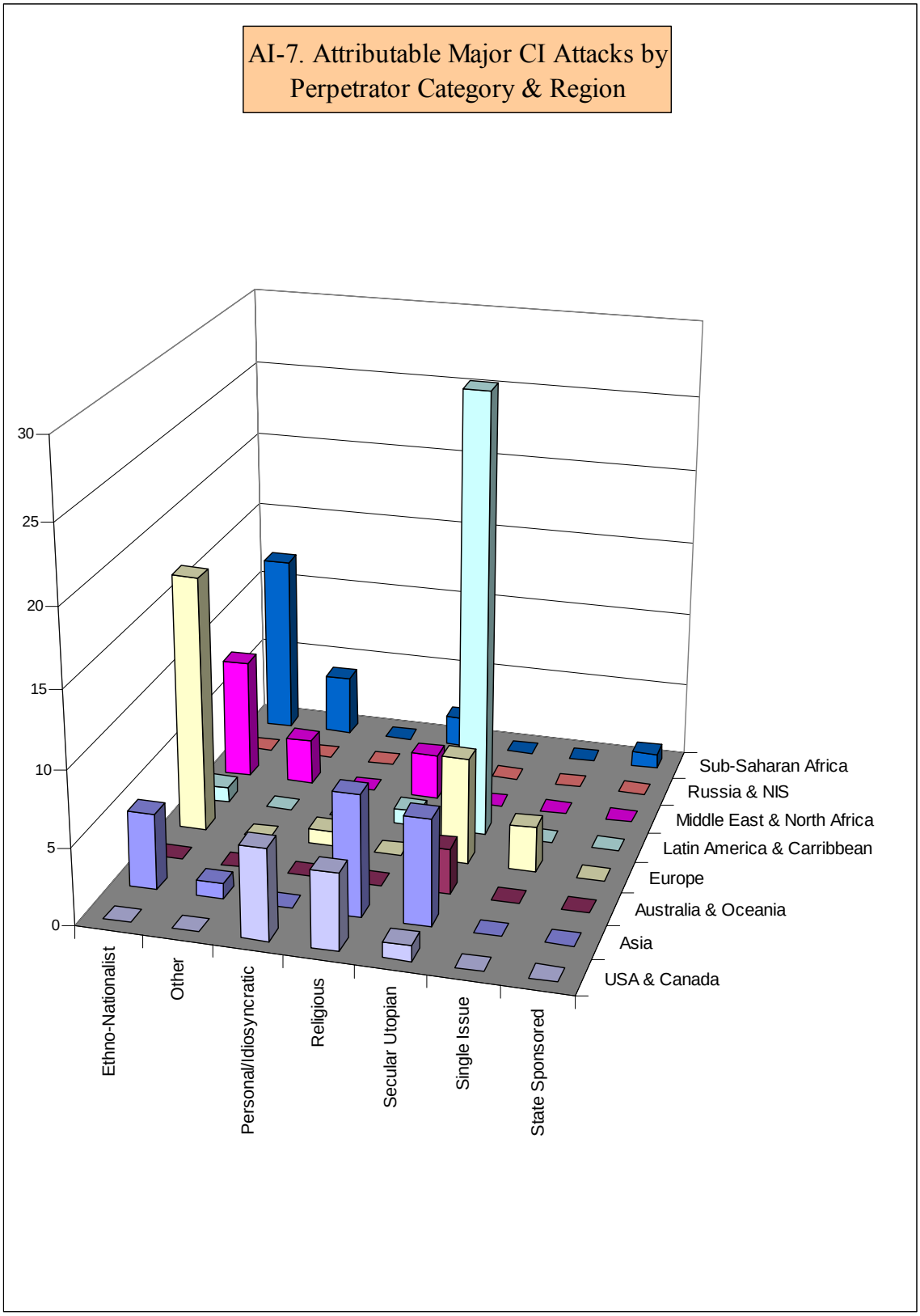
AI-4. Attributable Major and Minor CI Attacks by Perpetrator Category



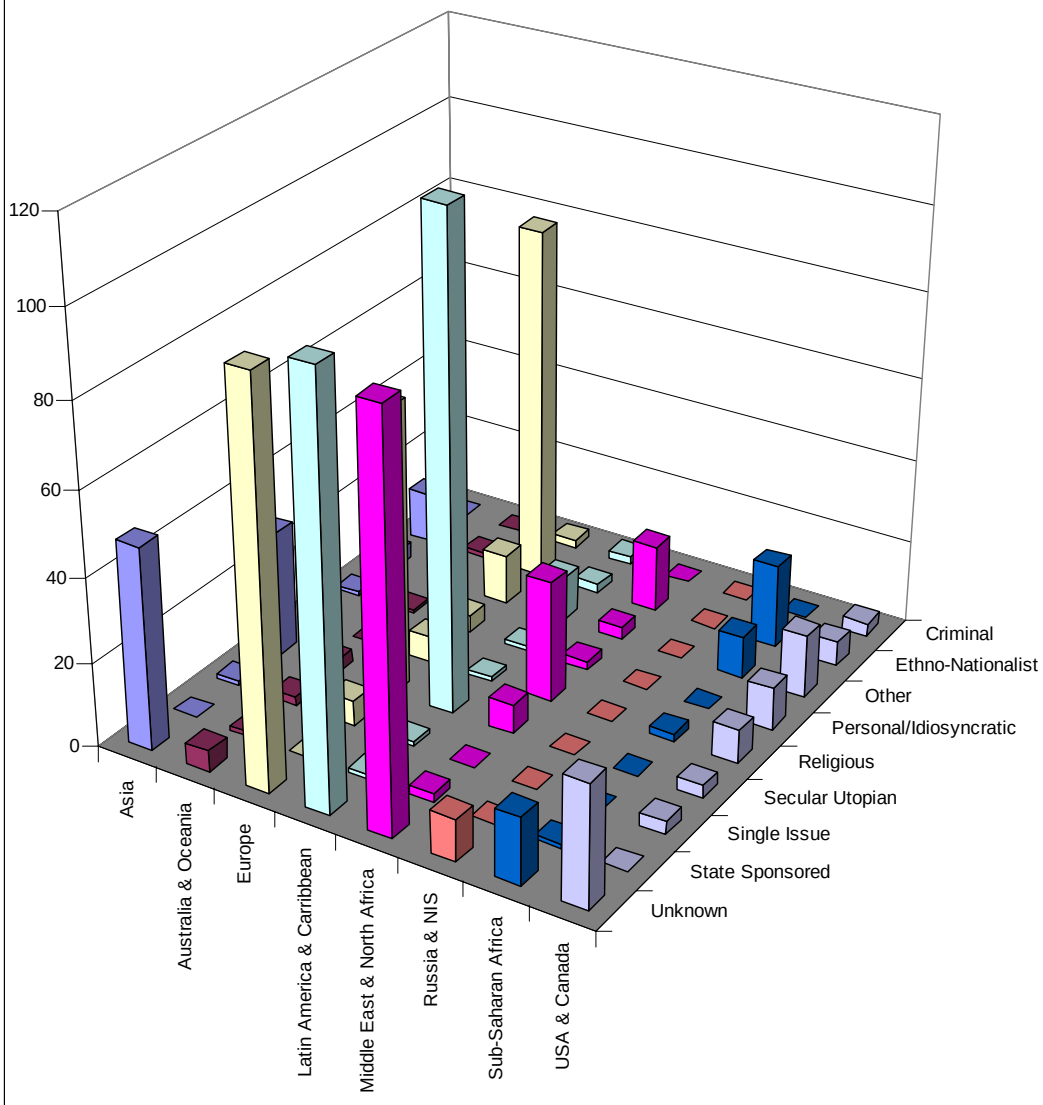

AI-5. Attributable Major CI Attacks by Perpetrator Category & Year
Ethnic/Nationalist/Separatist/Irredentist
Other
Personal/Idiosyncratic
Religious
Secular Utopian
Single Issue
0
1
2
3
4
5
6
7
8
9
1930
1940
1950
1960
1970
1980
1990
2000
2010


AI-6. Attributable Major & Minor CI Attacks by Perpetrator Category & Year
Criminal
Ethnic/Nationalist/Separatist/Irredentist
Other
Personal/Idiosyncratic
Religious
Secular Utopian
Single Issue
0
2
4
6
8
10
12
14
16
18
1920
1930
1940
1950
1960
1970
1980
1990
2000
2010

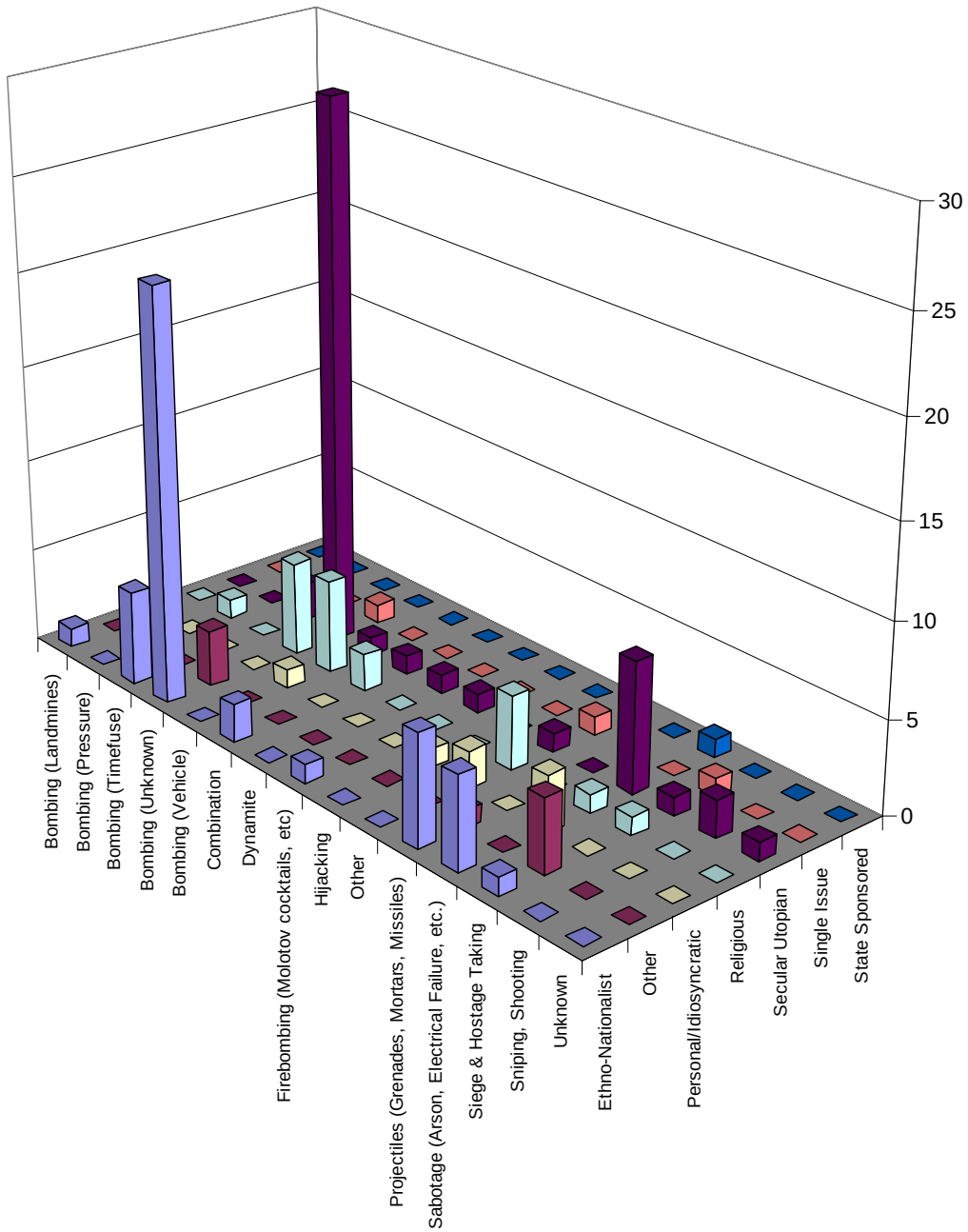
AI-7. Attributable Major CI Attacks by Perpetrator Category & Region

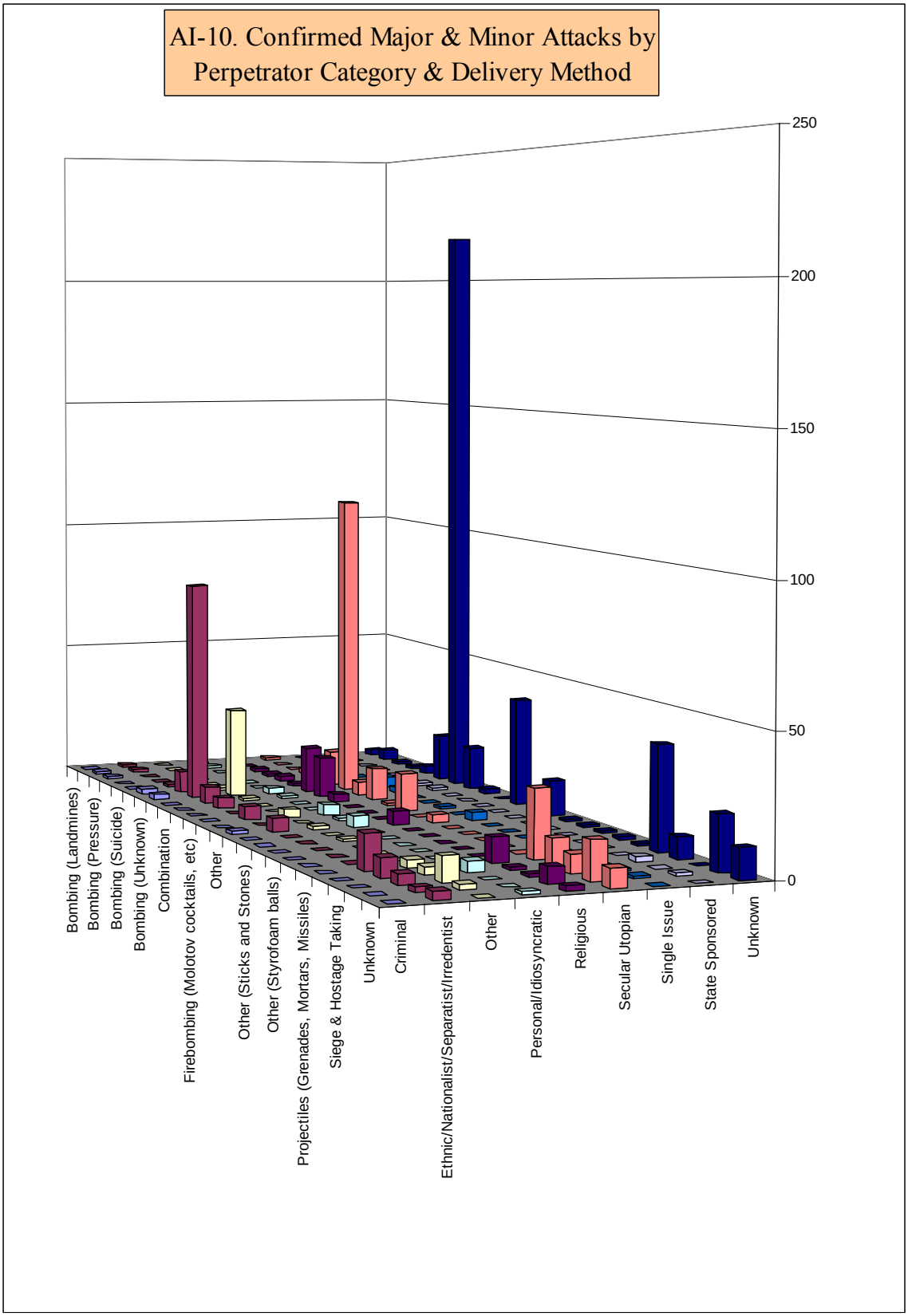


AI-8. Attributable Major & Minor CI Attacks by Perpetrator Category & Region

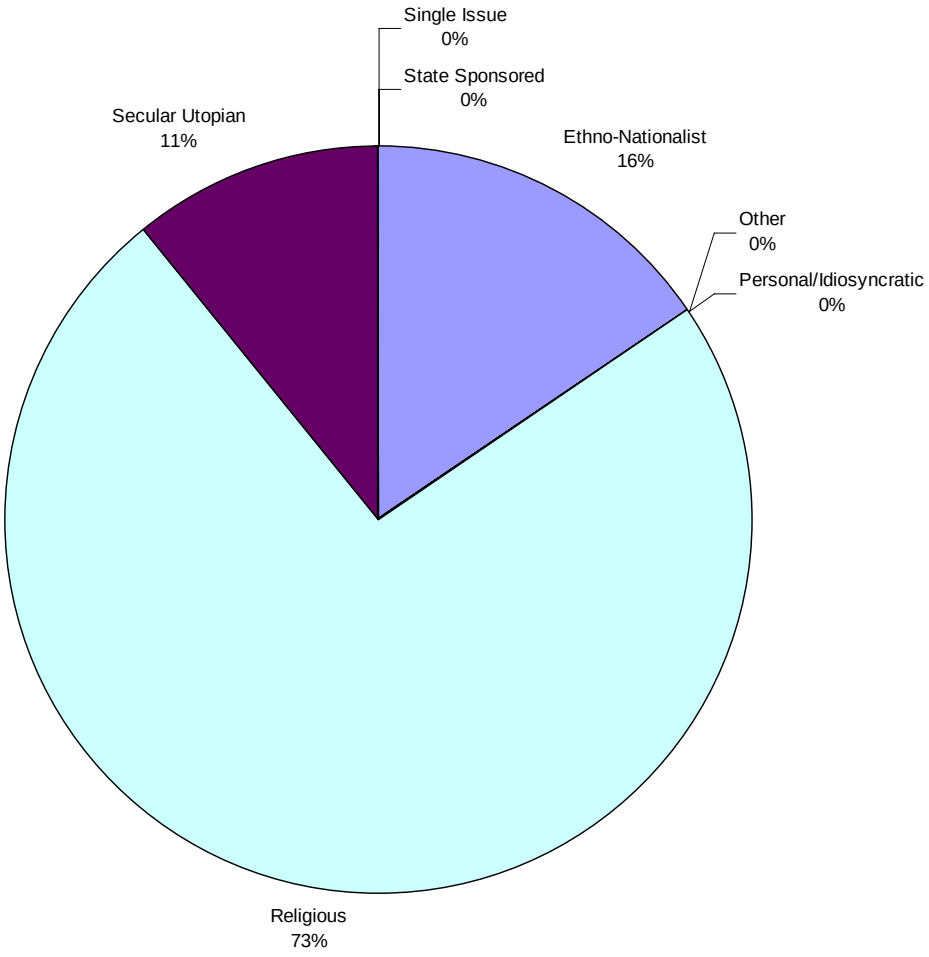


AI-9. Attributable Major CI Attacks by Perpetrator Category and Delivery Method

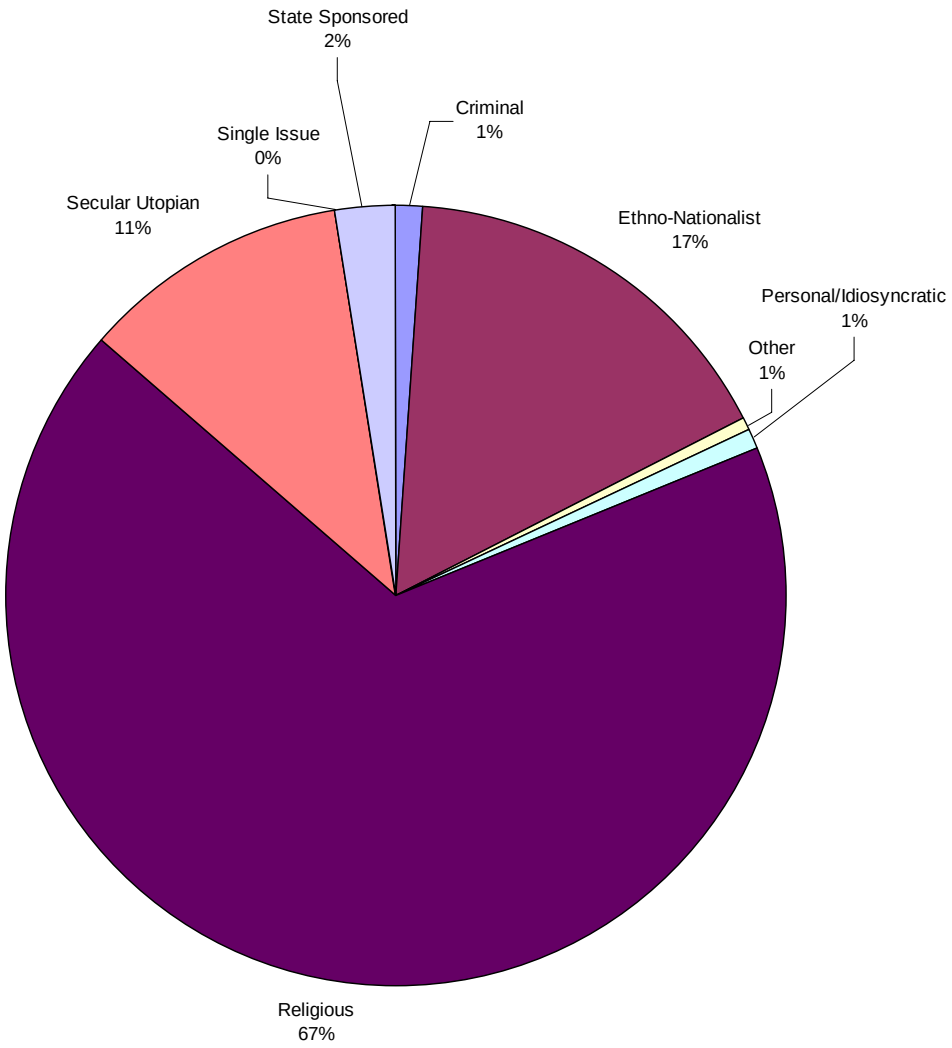



AI-10. Confirmed Major & Minor Attacks by Perpetrator Category & Delivery Method
250
200
150
100
50
0
Bombing (Landmines)
Bombing (Pressure)
Bombing (Suicide)
Bombing (Unknown)
Combination
Firebombing (Molotov cocktails, etc)
Other
Other (Sticks and Stones)
Other (Styrofoam balls)
Projectiles (Grenades, Mortars, Missiles)
Siege & Hostage Taking
Unknown
Criminal
Ethnic/Nationalist/Separatist/Irredentist
Other
Personal/Idiosyncratic
Religious
Secular Utopian
Single Issue
State Sponsored
Unknown

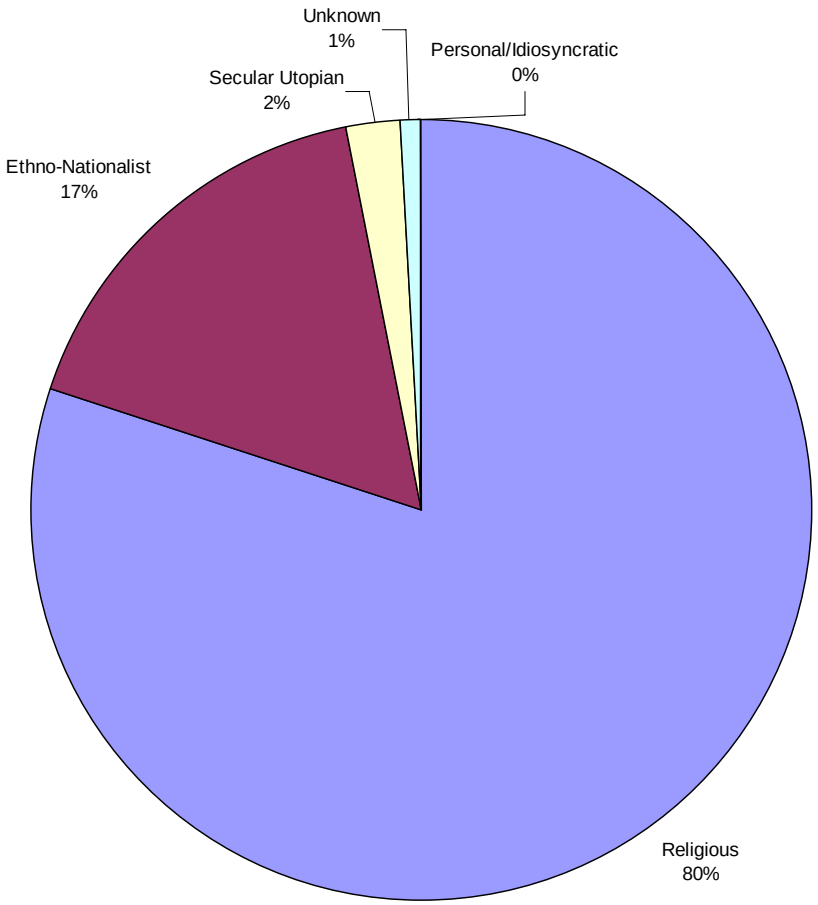
AI-11. Casualties Associated with Attributable Major CI Attacks by Perpetrator Category



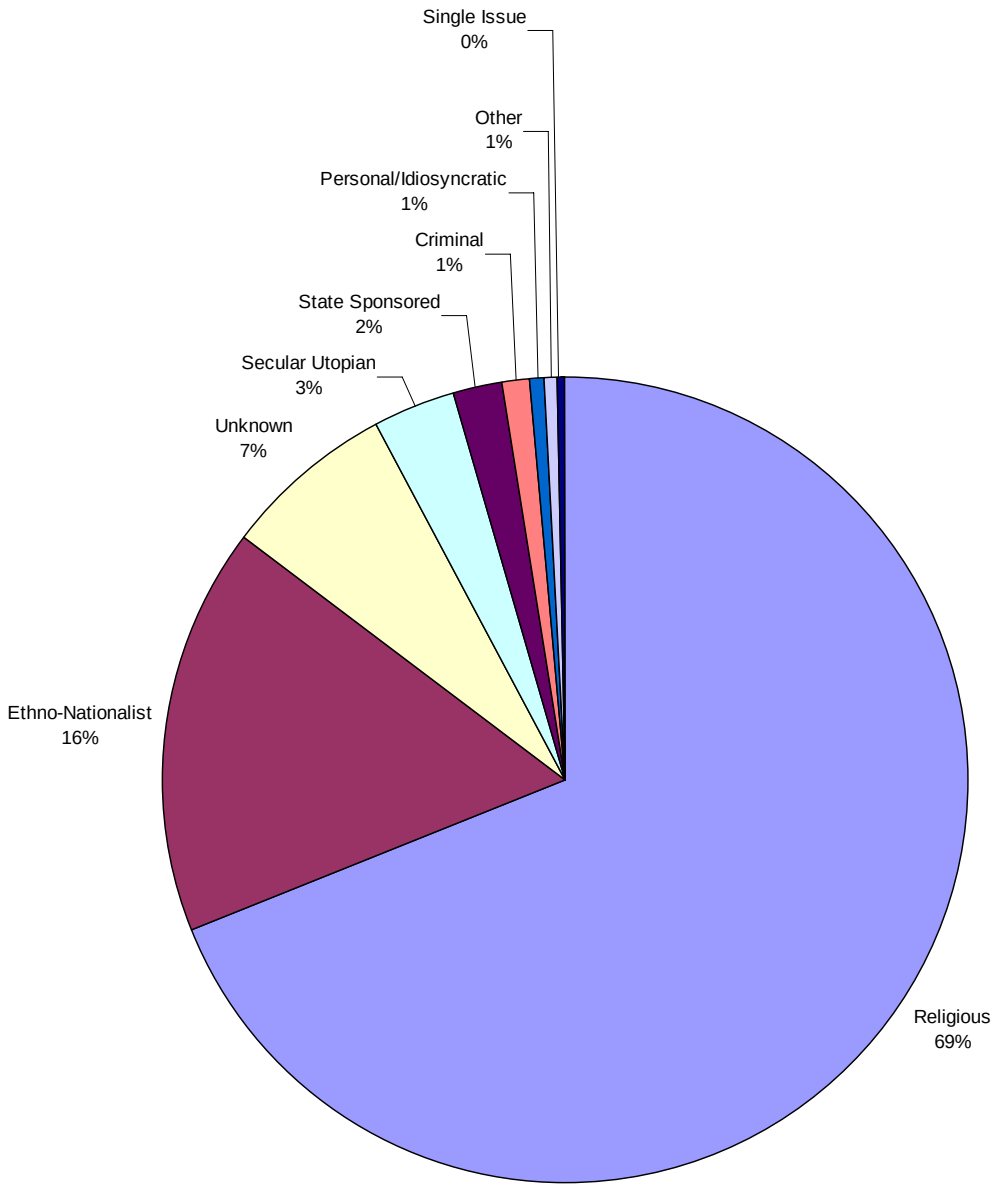
AI-12. Casulaties Associated with Attributable Major and Minor CI Attacks by Perpetrator Category



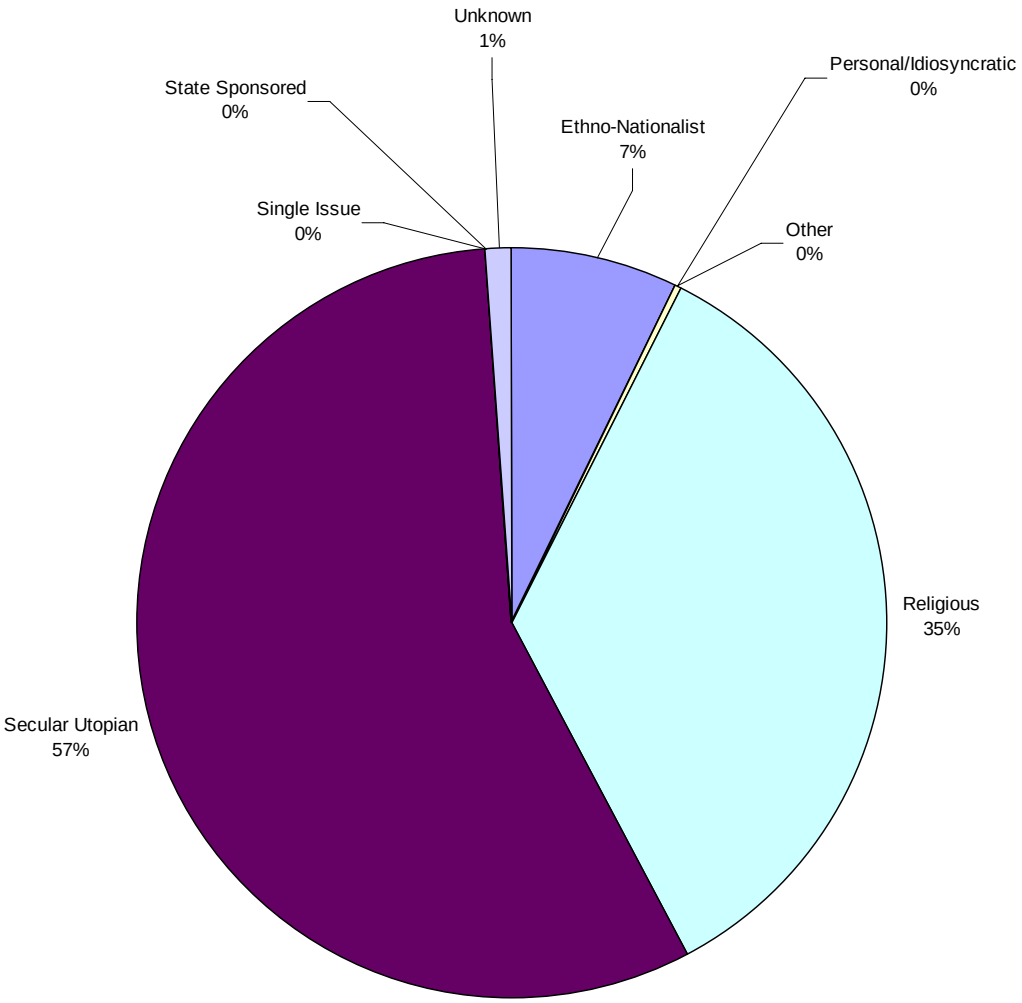
AI-13. Injuries Associated with Attributable Major CI Attacks by Perpetrator Category



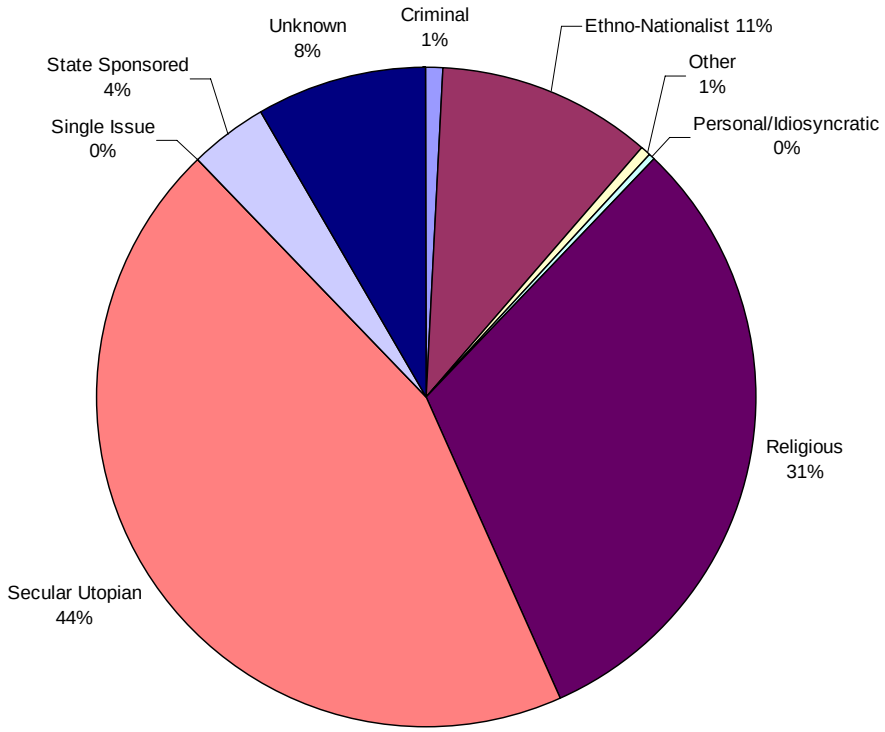
AI-14. Injuries Assocaited with Attributable Major & Minor CI Attacks by Perpetrator Category

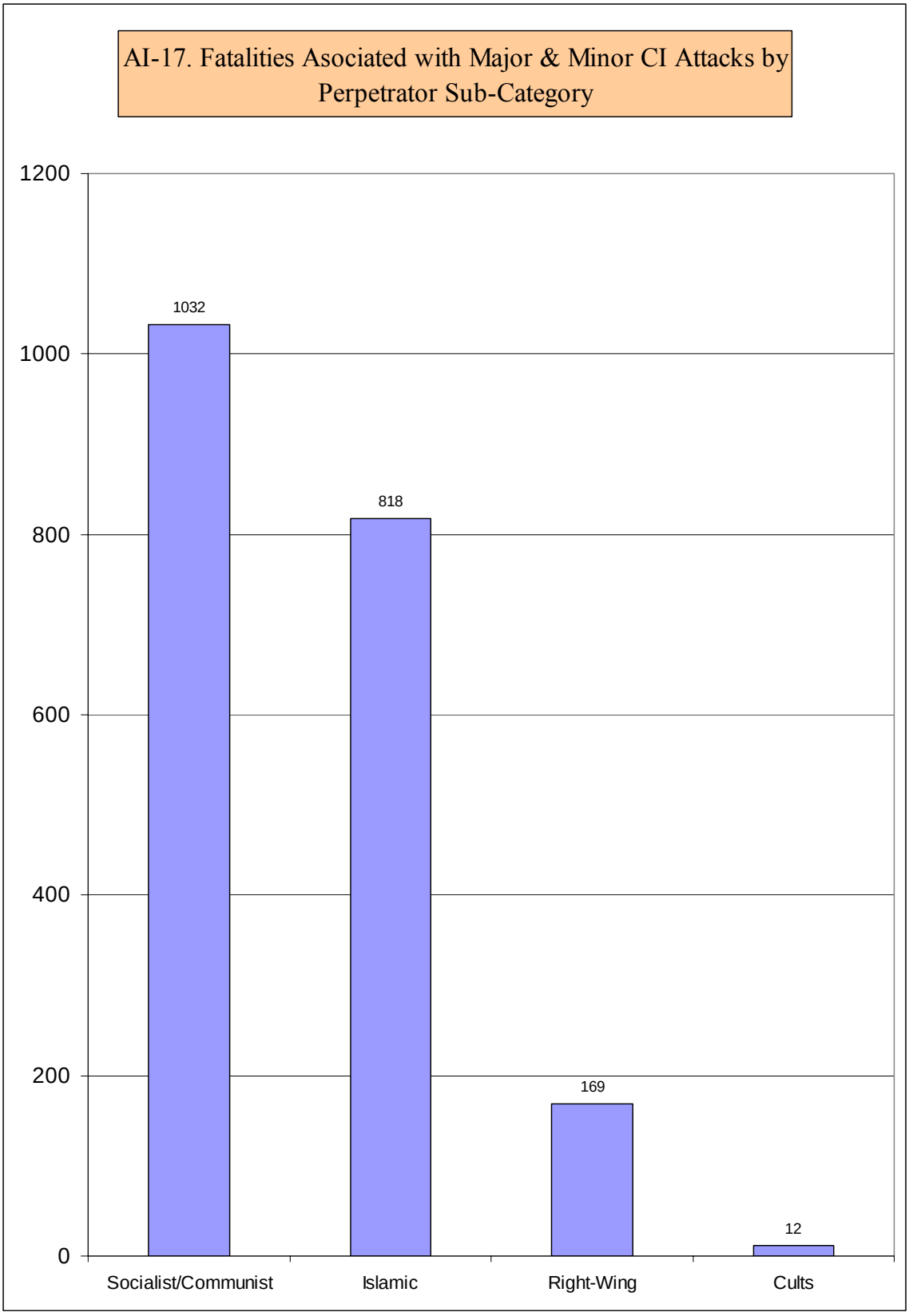


AI-15. Fatalities Associated with Attributable Major CI Attacks by Perpetrator Category

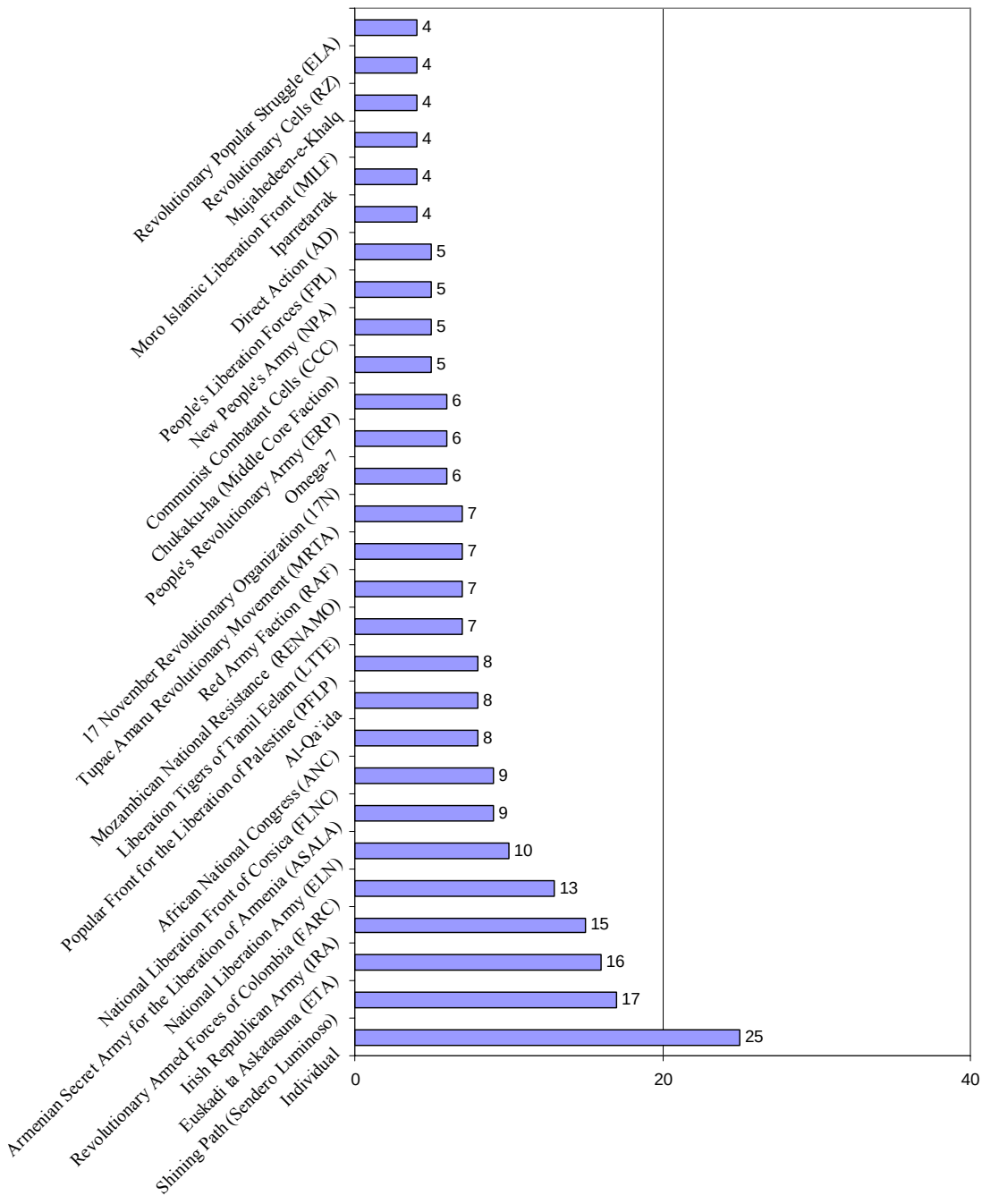


AI-16. Fatalities Associated with Attributable Major and Minor CI Attacks by Perpetrator Category

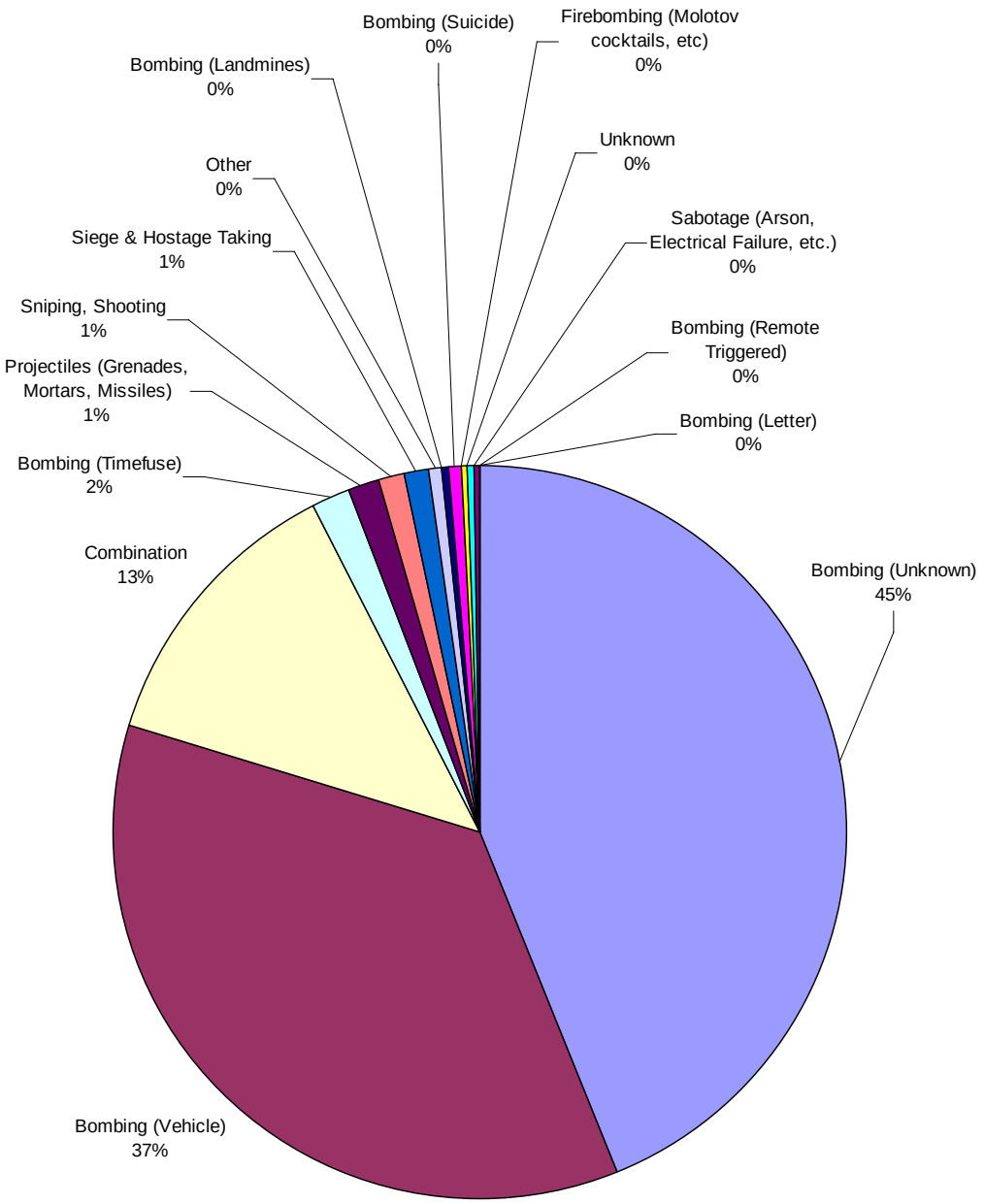



AI-17. Fatalities Asociated with Major & Minor CI Attacks by Perpetrator Sub-Category
1200
1000
800
600
400
200
0
1032
818
169
12
Socialist/Communist
Islamic
Right-Wing
Cults

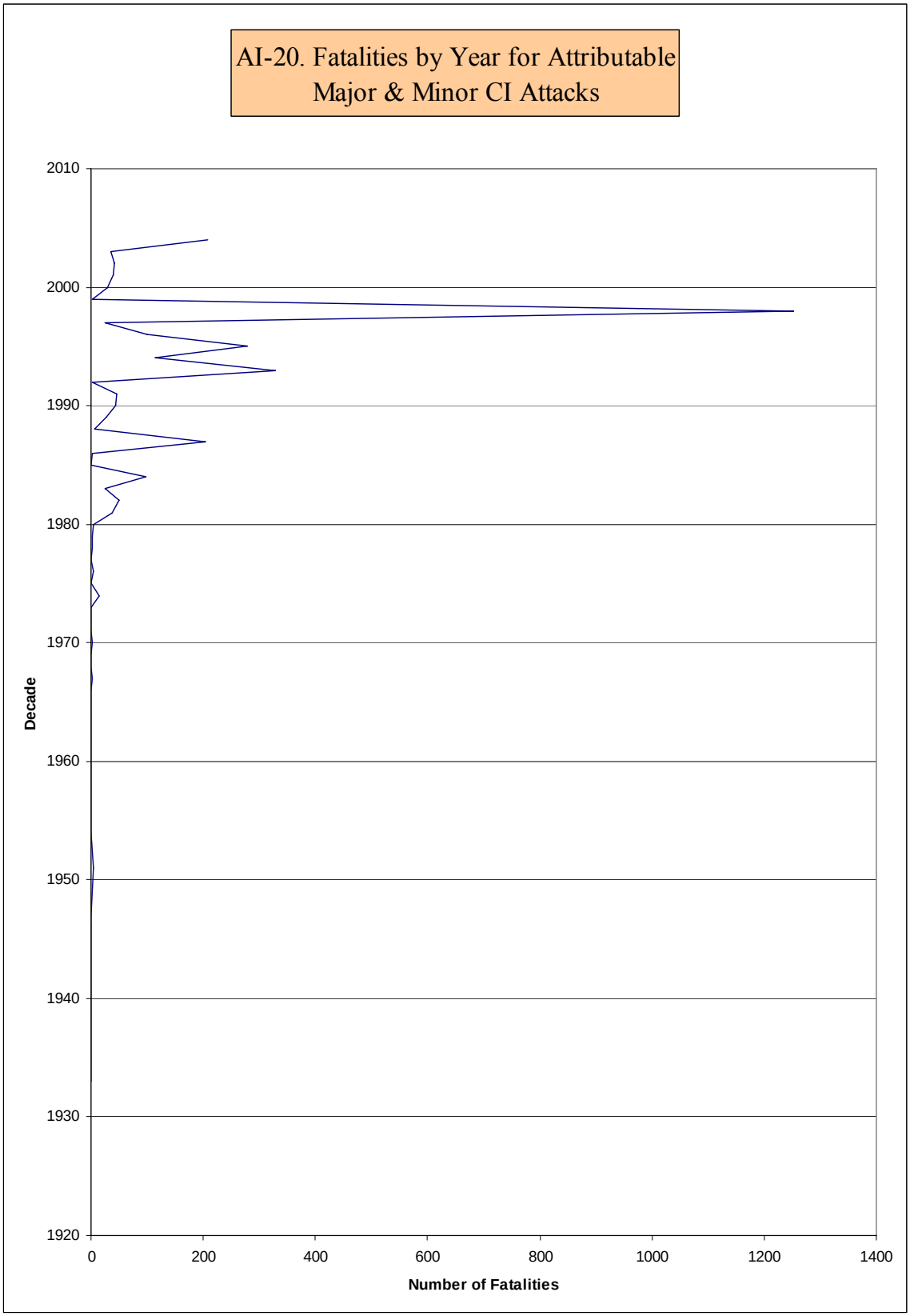
AI-18. Number of Major & Minor CI Attacks Attributable to Specific Groups



AI-19. Fatalities by Type of Attack/Delivery for Attributable Major and Minor CI Attacks



AI-20. Fatalities by Year for Attributable Major & Minor CI Attacks



Appendix II: DECIDe FRAMEWORK WORKSHEET*

*Note to User: This worksheet is designed to be used in conjunction with the analytical framework outlined in Chapter 5.

Step 1

DIRECTIONS: Consider group's inclination to attack CI based on known data.

1) Is there specific evidence that the group is planning to attack CI in the short / medium term?	YES _____ NO _____
2) Has the group attacked or made serious attempts to attack CI in the recent past?	YES _____ NO _____

IF EITHER QUESTION IS ANSWERED "YES" A PRESUMPTION OF INTENT TO ATTACK CRITICAL INFRASTRUCTURE SHOULD BE ASSUMED. NO FURTHER ANALYSIS IS REQUIRED.

IF BOTH QUESTIONS ARE ANSWERED "NO" PROCEED TO STEP TWO.

Step 2

DIRECTIONS: Collect additional information on group and its environment. Refer to Figure 5.3 for questions to guide data collection. When data is gathered proceed to Step 3.

Step 3

DIRECTIONS: Follow the DECIDe Framework analysis process detailed in Chapter 5. Insight or information gained from consideration of each factor may be recorded in the spaces provided below. Where "Attractiveness" or "Capability" is measured, record identified values in spaces on the left-hand side of the page. To facilitate final "Determination of Intent" at the conclusion of the framework, it is recommended that a brief note justifying each value determination be recorded.

For consistency, [A] is used to denote the "Attractiveness" to the group of attacking critical infrastructure targets and [C] to denote the terrorist's perceived "Capability" to engage in a serious attack against critical infrastructure targets. Increases or decreases are represented by "+" or "-" signs as follows:

Some Increase:	+	Some Decrease:	-
Significant Increase:	+ +	Significant Decrease:	- -
Large Increase:	+ + +	Large Decrease:	- - -
Varying Increase: *(Dependent on Characteristics of Variable)*	+ . . .	Varying Decrease: *(Dependent on Characteristics of Variable)*	- . . .

* The DECIDe Framework worksheet was developed by Kevin S. Moran and Andrew Jayne.

3.1 Ideology

	Attractiveness	Rationale for Value Selection
1.	____	_____
		_____
2.	____	_____
		_____
3.	____	_____
		_____

3.2 Organizational Structure

	Capability	Rationale for Value Selection
1.	____	_____
		_____
2.	____	_____
		_____

3.3 Organizational Dynamics

Data Requirement Notes

_____

_____

_____

_____

3.4 Demographics

Attractiveness Rationale for Value Selection

1. ____ _____

_____

_____

_____

3.5 Resources

Data Requirement Notes

_____

_____

_____

_____

3.6 Operational Capabilities

Capability Rationale for Value Selection

1. ____ _____

_____

2. ____ _____

_____

3. ____ _____

_____

4. ____ _____

_____

3.7 ***External Relations: Sympathizers / Supporters***

Attractiveness Rationale for Value Selection

1. ____ _____

_____

External Relations: State Sponsors

Capability Rationale for Value Selection

1a. ____ _____

_____

Attractiveness

1b. ____ _____

_____

External Relations: State Apparatus

Attractiveness Rationale for Value Selection

1. ____ _____

_____

External Relations: Criminal and Other Extremist Groups

Attractiveness Rationale for Value Selection

1. ____ _____

_____

External Relations: Media

Attractiveness Rationale for Value Selection

1a. ____ _____

Capability

1b. ____ _____

_____

3.8 ***Critical Infrastructure Characteristics***

Data Requirement Notes

_____

_____

_____

_____

3.9 ***General Planning Characteristics***

Data Requirement Notes

_____

_____

_____

3.10 ***Perceptual Filter***

Data Requirement Notes

_____

_____

_____

_____

Step 4

DIRECTIONS: Evaluate group's operational objectives using the data recorded above and the process found on pages 145 – 148. Record identified operational objectives in the space below.

Operational Objective Notes

_____

_____

_____

_____

4.1 Operational Objectives Analysis

1) Do CI targets fall within group's operational objectives?	YES _____ NO _____

IF ANSWER IS "YES" PROCEED TO CAPABILITIES ANALYSIS.

IF ANSWER IS "NO" PRUSUMPTION IS GROUP WILL NOT ATTACK CRITICAL INFRASTRUCTURE. NO FURTHER ANALYSIS REQUIRED.

4.2 Capabilities Analysis

1) Does available data indicate group preference to attack particular CI type(s)?	YES _____ NO _____

IF ANSWER IS "YES" USE TABLE 5.2 AND ACCOMPANYING EXPLANATION OF VARIABLES TO DETERMINE IF GROUP HAS CAPABILITIES NECESSARY TO CONDUCT ATTACK AGAINST THE SPECIFIC INFRASTRUCTURE TYPE. (Identify values from Framework Table 5.2)

IF ANSWER IS "NO" USE TABLE 5.2 AND ACCOMPANYING EXPLANATION OF VARIABLES TO DETERMINE IF GROUP HAS CAPABILITIES NECESSARY TO CONDUCT A "GENERAL" CRITICAL INFRASTRUCTURE ATTACK.

Capabilities Required to Conduct Major CI Attack

ASSESSMENT CATEGORIES	MINIMUM ATTACK REQUIREMENTS FOR SPECIFIC INFRASTRUCTURE *(See Table 5.2)* Infrastructure:_____	MINIMUM ATTACK REQUIREMENTS FOR CI IN GENERAL		OBSERVED / INFERRED TERRORIST GROUP CAPABILITIES
PROTECTION LEVEL		**HIGH**	**LOW**	
PHYSICAL REQUIREMENTS		Medium	Low	
WEAPONS		Medium	Low - Medium	
FINANCIAL RESOURCES		Low	Low	
LOGISITICAL RESOURCES		Medium	Low	
ABILITY TO INNOVATE		Medium	Low	
TECHNOLOGY LEVEL		Medium	Medium	
SKILL SET		Medium	Medium	
FAMILIARITY w/ TARGET ENVIRONMENT		High	Medium	
COMMUNICATIONS		Medium	Medium	

Capabilities Analysis Notes

TO CONFIRM ANALYSIS, REVIEW PREVIOUSLY IDENTIFIED “CAPABILITY” [“C”] VALUES AND AMALGAMATE IDENTIFIED INDICATORS TO: 1) CONFIRM THE PERCEIVED CAPABILITIES THRESHOLD; 2) ARGUE FOR ANALYST REEVALUATION, OR; 3) PROVIDE AN ALTERNATIVE EXPLANATORY MECHANISM IF DATA IS STILL INSUFFICIENT.

Final Determination Notes

Appendix III: STATISTICAL ANALYSIS RESULTS*

This appendix contains output from the statistical analysis performed on the CrITIC dataset. These findings are the basis for the discussion found in Chapter 4.

A. Two-Way ANOVA Test between the Types of Terrorist Categories and the Number of Attacks over Decades

Univariate Analysis of Variance

Between-Subjects Factors

		Value Label	N
PERPCAT	1	Criminal	51
	2	Ethnic/Nationalist/Separatist	51
	3	Other	51
	4	Personal/Idiosyncratic	51
	5	Religious	51
	6	Secular/Utopian	51
	7	Single Issue	51
	8	State Sponsored	51
	9	Unknown	51
YEAR	1	1960s and before	144
	2	1970s	90
	3	1980s	90
	4	1990s	90
	5	2000s	45

* This appendix was prepared by Sean Lucas and Sundara Vadlamudi.

Descriptive Statistics

Dependent Variable: # of attacks(perpcat) all cases

PERPCAT	YEAR	Mean	Std. Deviation	N
Criminal	1960s and before	.0000	.0000	16
	1970s	.0000	.0000	10
	1980s	.2000	.4216	10
	1990s	.4000	.9661	10
	2000s	.2000	.4472	5
	Total	.1373	.4907	51
Ethnic/Nationalist/Separatist	1960s and before	.8125	1.2764	16
	1970s	1.2000	1.3984	10
	1980s	7.9000	5.8585	10
	1990s	4.6000	3.1693	10
	2000s	2.2000	1.9235	5
	Total	3.1569	4.0810	51
Other	1960s and before	.5625	1.5478	16
	1970s	1.4000	1.6465	10
	1980s	2.0000	2.1082	10
	1990s	1.8000	1.3984	10
	2000s	1.0000	1.2247	5
	Total	1.2941	1.6768	51
Personal/Idiosyncratic	1960s and before	.0000	.0000	16
	1970s	.0000	.0000	10
	1980s	.9000	.9944	10
	1990s	.4000	.8433	10
	2000s	1.4000	2.0736	5
	Total	.3922	.9398	51
Religious	1960s and before	.1250	.3416	16
	1970s	1.000E-01	.3162	10
	1980s	3.2000	2.4855	10
	1990s	3.1000	2.3310	10
	2000s	5.2000	4.3818	5
	Total	1.8039	2.6534	51
Secular/Utopian	1960s and before	.9375	2.0156	16
	1970s	3.7000	3.4976	10
	1980s	16.1000	5.0651	10
	1990s	6.2000	3.7947	10
	2000s	6.0000	7.5498	5
	Total	5.9804	6.6977	51
Single Issue	1960s and before	6.250E-02	.2500	16
	1970s	.1000	.3162	10
	1980s	.6000	.8433	10
	1990s	.3000	.6749	10
	2000s	.8000	1.7889	5
	Total	.2941	.7562	51
State Sponsored	1960s and before	.0000	.0000	16
	1970s	.0000	.0000	10
	1980s	.6000	.6992	10
	1990s	.3000	.4830	10
	2000s	.0000	.0000	5
	Total	.1765	.4339	51
Unknown	1960s and before	1.6250	1.9958	16
	1970s	4.7000	2.5408	10
	1980s	15.5000	8.4623	10
	1990s	13.7000	13.1407	10
	2000s	9.2000	9.8843	5
	Total	8.0588	9.3390	51
Total	1960s and before	.4583	1.2565	144
	1970s	1.2444	2.2848	90
	1980s	5.2222	7.2076	90
	1990s	3.4222	6.1935	90
	2000s	2.8889	5.1178	45
	Total	2.3660	4.9813	459

Levene's Test of Equality of Error Variances [a]

Dependent Variable: # of attacks(perpcat) all cases

F	df1	df2	Sig.
9.537	44	414	.000

Tests the null hypothesis that the error variance of the dependent variable is equal across groups.

a. Design: Intercept+PERPCAT+YEAR+PERPCAT * YEAR

Tests of Between-Subjects Effects

Dependent Variable: # of attacks(perpcat) all cases

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	7058.760[a]	44	160.426	15.425	.000
Intercept	2803.114	1	2803.114	269.521	.000
PERPCAT	3525.647	8	440.706	42.374	.000
YEAR	1484.182	4	371.046	35.676	.000
PERPCAT * YEAR	2233.441	32	69.795	6.711	.000
Error	4305.750	414	10.400		
Total	13934.000	459			
Corrected Total	11364.510	458			

a. R Squared = .621 (Adjusted R Squared = .581)

B. Multiple Discriminant Analysis

Discriminant

Analysis Case Processing Summary

Unweighted Cases		N	Percent
Valid		1080	99.6
Excluded	Missing or out-of-range group codes	0	.0
	At least one missing discriminating variable	0	.0
	Both missing or out-of-range group codes and at least one missing discriminating variable	4	.4
	Total	4	.4
Total		1084	100.0

Group Statistics

ATTTYPE		Mean	Std. Deviation	Valid N (listwise) Unweighted	Weighted
1	infrastructure attacked(perpcat) major confirmed cases	8.28	4.15	680	680.000
	SUCATT	1.01	.12	680	680.000
	claim of responsibility all cases	1.26	.44	680	680.000
	YEAR	3.20	.99	680	680.000
2	infrastructure attacked(perpcat) major confirmed cases	8.17	4.36	24	24.000
	SUCATT	1.08	.28	24	24.000
	claim of responsibility all cases	1.50	.51	24	24.000
	YEAR	3.50	.93	24	24.000
3	infrastructure attacked(perpcat) major confirmed cases	12.00	.[a]	1	1.000
	SUCATT	1.00	.[a]	1	1.000
	claim of responsibility all cases	1.00	.[a]	1	1.000
	YEAR	5.00	.[a]	1	1.000
4	infrastructure attacked(perpcat) major confirmed cases	6.30	3.18	80	80.000
	SUCATT	1.00	.00	80	80.000
	claim of responsibility all cases	1.11	.32	80	80.000
	YEAR	3.09	.70	80	80.000
5	infrastructure attacked(perpcat) major confirmed cases	13.00	.[a]	1	1.000
	SUCATT	1.00	.[a]	1	1.000
	claim of responsibility all cases	1.00	.[a]	1	1.000
	YEAR	5.00	.[a]	1	1.000
6	infrastructure attacked(perpcat) major confirmed cases	7.55	4.67	42	42.000
	SUCATT	1.00	.00	42	42.000
	claim of responsibility all cases	1.10	.30	42	42.000
	YEAR	3.90	1.08	42	42.000
7	infrastructure attacked(perpcat) major confirmed cases	6.42	3.18	101	101.000
	SUCATT	1.00	.00	101	101.000
	claim of responsibility all cases	1.19	.39	101	101.000
	YEAR	3.39	.86	101	101.000
8	infrastructure attacked(perpcat) major confirmed cases	9.51	3.93	41	41.000
	SUCATT	1.02	.16	41	41.000
	claim of responsibility all cases	1.34	.48	41	41.000
	YEAR	3.61	1.02	41	41.000
9	infrastructure attacked(perpcat) major confirmed cases	6.54	2.83	24	24.000
	SUCATT	1.00	.00	24	24.000
	claim of responsibility all cases	1.38	.49	24	24.000
	YEAR	3.88	.85	24	24.000
10	infrastructure attacked(perpcat) major confirmed cases	7.05	3.82	57	57.000
	SUCATT	1.00	.00	57	57.000
	claim of responsibility all cases	1.19	.40	57	57.000
	YEAR	3.42	1.03	57	57.000
11	infrastructure attacked(perpcat) major confirmed cases	9.31	5.76	29	29.000
	SUCATT	1.00	.00	29	29.000
	claim of responsibility all cases	1.17	.38	29	29.000
	YEAR	4.10	1.14	29	29.000
Total	infrastructure attacked(perpcat) major confirmed cases	7.91	4.11	1080	1080.000
	SUCATT	1.01	.11	1080	1080.000
	claim of responsibility all cases	1.24	.43	1080	1080.000
	YEAR	3.31	.99	1080	1080.000

a. Insufficient data

Tests of Equality of Group Means

	Wilks' Lambda	F	df1	df2	Sig.
infrastructure attacked(perpcat) major confirmed cases	.955	5.076	10	1069	.000
SUCATT	.986	1.533	10	1069	.122
claim of responsibility all cases	.972	3.128	10	1069	.001
YEAR	.939	6.955	10	1069	.000

Box's Test of Equality of Covariance Matrices

Log Determinants

ATTTYPE	Rank	Log Determinant
1	4	-3.150
2	4	-1.848
3	.[a]	.[b]
4	3	.[c]
5	.[a]	.[b]
6	3	.[c]
7	3	.[c]
8	4	-2.538
9	3	.[c]
10	3	.[c]
11	3	.[c]
Pooled within-groups	4	-3.513

The ranks and natural logarithms of determinants printed are those of the group covariance matrices.

a. Rank < 1

b. Too few cases to be non-singular

c. Singular

Test Results[a]

Box's M		87.038
F	Approx.	4.133
	df1	20
	df2	16220.583
	Sig.	.000

Tests null hypothesis of equal population covariance matrices.

a. Some covariance matrices are singular and the usual procedure will not work. The non-singular groups will be tested against their own pooled within-groups covariance matrix. The log of its determinant is -2.959.

Summary of Canonical Discriminant Functions

Eigenvalues

Function	Eigenvalue	% of Variance	Cumulative %	Canonical Correlation
1	.077[a]	49.6	49.6	.268
2	.052[a]	33.4	83.1	.223
3	.023[a]	14.6	97.6	.149
4	.004[a]	2.4	100.0	.061

a. First 4 canonical discriminant functions were used in the analysis.

Wilks' Lambda

Test of Function(s)	Wilks' Lambda	Chi-square	df	Sig.
1 through 4	.859	162.400	40	.000
2 through 4	.926	82.495	27	.000
3 through 4	.974	28.040	16	.031
4	.996	3.983	7	.782

Standardized Canonical Discriminant Function Coefficients

	Function			
	1	2	3	4
infrastructure attacked(perpcat) major confirmed cases	.529	.608	-.650	-.023
SUCATT	.251	.120	.439	.866
claim of responsibility all cases	.302	.366	.702	-.536
YEAR	-.880	.518	.144	.028

Structure Matrix

	Function			
	1	2	3	4
YEAR	-.729*	.677	.037	.099
infrastructure attacked(perpcat) major confirmed cases	.369	.768*	-.521	.050
claim of responsibility all cases	.339	.414	.680*	-.501
SUCATT	.243	.254	.406	.843*

Pooled within-groups correlations between discriminating variables and standardized canonical discriminant functions
Variables ordered by absolute size of correlation within function.

*. Largest absolute correlation between each variable and any discriminant function

Functions at Group Centroids

	Function			
ATTTYPE	1	2	3	4
1	.173	1.541E-02	-3.31E-02	-9.62E-03
2	.211	.442	.702	.245
3	-1.200	1.302	-.858	.236
4	-.127	-.487	-3.66E-02	6.990E-02
5	-1.069	1.453	-1.019	.230
6	-.720	.125	-.145	.109
7	-.330	-.244	.114	-1.75E-02
8	3.851E-02	.502	5.348E-04	-2.81E-02
9	-.625	.198	.476	-.240
10	-.275	-.125	2.495E-02	-2.62E-02
11	-.614	.564	-.272	7.088E-03

Unstandardized canonical discriminant functions evaluated at group means

C. One-Way ANOVA Test between the Number of Casualties and the Different Types of Attack

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
fatalities	1	680	3.6691	34.1291	1.3088	1.0994	6.2389	.00	741.00
	2	24	16.3750	57.6382	11.7653	-7.9635	40.7135	.00	275.00
	3	1	.0000	.	.	.	.	.00	.00
	4	80	.1125	.7115	954E-02	.583E-02	.2708	.00	6.00
	5	1	.0000	.	.	.	.	.00	.00
	6	42	5.7857	29.5045	4.5526	-3.4085	14.9800	.00	188.00
	7	101	.3960	2.1311	.2121	.467E-02	.8167	.00	20.00
	8	41	.1707	.5875	175E-02	.470E-02	.3562	.00	3.00
	9	24	1.4167	4.8357	.9871	-.6253	3.4586	.00	22.00
	10	57	.6140	1.8685	.2475	.1183	1.1098	.00	9.00
	11	29	.3103	.8906	.1654	.841E-02	.6491	.00	4.00
	Total	1080	3.0231	29.0644	.8844	1.2878	4.7585	.00	741.00
injuries	1	680	17.3118	180.8109	6.9338	3.6975	30.9260	.00	4000.00
	2	24	67.3750	293.1098	59.8308	-56.3944	191.1444	.00	1440.00
	3	1	.0000	.	.	.	.	.00	.00
	4	80	1.1125	6.9099	.7725	-.4252	2.6502	.00	60.00
	5	1	.0000	.	.	.	.	.00	.00
	6	42	27.1429	160.2252	24.7233	-22.7868	77.0726	.00	1038.00
	7	101	.7624	2.7682	.2754	.2159	1.3089	.00	18.00
	8	41	3.3902	13.3321	2.0821	-.8179	7.5984	.00	78.00
	9	24	6.2500	24.6140	5.0243	-4.1436	16.6436	.00	120.00
	10	57	1.3509	3.5076	.4646	.4202	2.2816	.00	17.00
	11	29	1.5172	3.8043	.7064	.015E-02	2.9643	.00	17.00
	Total	1080	13.9861	153.3913	4.6675	4.8276	23.1446	.00	4000.00
total number of casu	1	680	20.9809	198.0152	7.5935	6.0713	35.8905	.00	4213.00
	2	24	83.7500	315.4252	64.3859	-49.4424	216.9424	.00	1523.00
	3	1	.0000	.	.	.	.	.00	.00
	4	80	1.2250	7.5624	.8455	-.4579	2.9079	.00	66.00
	5	1	.0000	.	.	.	.	.00	.00
	6	42	32.9286	165.9151	25.6013	-18.7742	84.6314	.00	1050.00
	7	101	1.1584	4.2420	.4221	.3210	1.9958	.00	34.00
	8	41	3.5610	13.5979	2.1236	-.7310	7.8530	.00	79.00
	9	24	7.6667	29.0960	5.9392	-4.6195	19.9528	.00	142.00
	10	57	1.9649	4.8512	.6426	.6777	3.2521	.00	23.00
	11	29	1.8276	4.0889	.7593	.2722	3.3829	.00	17.00
	Total	1080	17.0093	167.5169	5.0974	7.0074	27.0112	.00	4213.00

Test of Homogeneity of Variances

	Levene Statistic	df1	df2	Sig.
fatalities	2.628	10	1069	.004
injuries	1.831	10	1069	.051
total number of casualties	2.318	10	1069	.011

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
fatalities	Between Groups	7215.674	10	721.567	.853	.577
	Within Groups	04258.748	1069	845.892		
	Total	11474.421	1079			
injuries	Between Groups	34159.353	10	13415.935	.568	.841
	Within Groups	25253513	1069	23623.492		
	Total	25387673	1079			
total number of casualtie	Between Groups	03254.956	10	20325.496	.722	.704
	Within Groups	30075547	1069	28134.282		
	Total	30278802	1079			

D. One-Way ANOVA Test between the Types of Terrorist Groups and the Number of Casualties

Descriptives

		N	Mean	Std. Deviation	Std. Erro	% Confidence Inte for Mean		Minimum	Maximun
						Lower Bound	Upper Bound		
fatalities	Criminal	7	2.4286	6.4254	2.4286	-3.5139	8.3711	.00	17.00
	Ethnic/Nationalist/	162	2.3580	12.3417	.9697	.4431	4.2729	.00	115.00
	Other	66	3.1667	20.9847	2.5830	-1.9920	8.3253	.00	169.00
	Personal/Idiosync	19	.3684	1.3829	.3172	-.2981	1.0349	.00	6.00
	Religious	91	3.7143	48.4661	5.0806	3.6207	23.8078	.00	317.00
	Secular/Utopian	300	3.6667	45.5886	2.6321	-1.5130	8.8464	.00	741.00
	Single Issue	15	67E-02	.2582	67E-02	32E-02	.2097	.00	1.00
	State Sponsored	9	0.8889	31.9235	0.6412	13.6497	35.4275	.00	96.00
	Unknown	411	.4939	2.7125	.1338	.2309	.7569	.00	32.00
	Total	1080	3.0231	29.0644	.8844	1.2878	4.7585	.00	741.00
injuries	Criminal	7	6.4286	43.4659	6.4286	-23.7707	56.6278	.00	115.00
	Ethnic/Nationalist/	162	4.0556	14.9014	9.0275	-3.7720	31.8832	.00	440.00
	Other	66	9.0758	61.6133	7.5841	-6.0707	24.2222	.00	500.00
	Personal/Idiosync	19	5.1053	17.9811	4.1252	-3.5614	13.7719	.00	78.00
	Religious	91	4.7912	92.7062	1.6496	2.1802	17.4022	.00	000.00
	Secular/Utopian	300	1.5367	8.5247	.4922	.5681	2.5052	.00	100.00
	Single Issue	15	1.2000	2.3664	.6110	-.1105	2.5105	.00	7.00
	State Sponsored	9	6.5556	76.7123	5.5708	-32.4107	35.5219	.00	231.00
	Unknown	411	2.0754	10.4102	.5135	1.0660	3.0848	.00	150.00
	Total	1080	3.9861	53.3913	4.6675	4.8276	23.1446	.00	000.00
total number of c	Criminal	7	8.8571	49.8913	8.8571	-27.2846	64.9989	.00	132.00
	Ethnic/Nationalist/	162	6.4136	23.0849	9.6705	-2.6837	35.5109	.00	523.00
	Other	66	2.2424	32.5078	0.1560	-8.0405	32.5254	.00	669.00
	Personal/Idiosync	19	5.4737	18.2006	4.1755	-3.2987	14.2461	.00	79.00
	Religious	91	8.5055	28.2251	5.3730	18.4973	38.5137	.00	213.00
	Secular/Utopian	300	5.2033	52.9590	3.0576	-.8138	11.2205	.00	841.00
	Single Issue	15	1.2667	2.3745	.6131	27E-02	2.5816	.00	7.00
	State Sponsored	9	7.4444	08.6337	6.2112	-46.0588	20.9477	.00	327.00
	Unknown	411	2.5693	12.1864	.6011	1.3877	3.7510	.00	175.00
	Total	1080	7.0093	67.5169	5.0974	7.0074	27.0112	.00	213.00

Test of Homogeneity of Variances

	Levene Statistic	df1	df2	Sig.
fatalities	5.471	8	1071	.000
injuries	18.502	8	1071	.000
total number of casualties	18.379	8	1071	.000

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
fatalities	Between Groups	14052.090	8	1756.511	2.096	.034
	Within Groups	97422.332	1071	837.929		
	Total	11474.421	1079			
injuries	Between Groups	1036521.3	8	29565.157	5.698	.000
	Within Groups	24351152	1071	22736.836		
	Total	25387673	1079			
total number of casualtie	Between Groups	1270355.6	8	58794.454	5.863	.000
	Within Groups	29008446	1071	27085.384		
	Total	30278802	1079			

E. One-Way ANOVA Test between the Type of Infrastructure Attacked and the number of Fatalities, Injuries, and Casualties.

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
fatalities	Avaition Infra	25	2.1600	7.3862	1.4772	-.8889	5.2089	.00	32.00
	Chemical Plant	9	2.1111	5.6224	1.8741	-2.2106	6.4329	.00	17.00
	Comm. Infra	5	.8000	1.7889	.8000	-1.4212	3.0212	.00	4.00
	Damns & Wat.	12	5.1667	17.2723	4.9861	-5.8076	16.1410	.00	60.00
	Embass/Cons.	491	.6069	9.6505	.4355	-.2488	1.4626	.00	213.00
	Finan Inst.	121	1.3306	8.5755	.7796	-.2130	2.8741	.00	83.00
	Food Stor Facil.	1	.0000	.	.	.	.	.00	.00
	Hospitals	10	2.1000	3.3813	1.0693	-.3189	4.5189	.00	10.00
	Mil. Bases and Pol. St.	12	2.2500	6.0321	1.7413	-1.5826	6.0826	.00	21.00
	Oil/Gas	94	8.3617	76.4172	7.8818	-7.2901	24.0135	.00	741.00
	Other	9	26.4444	61.9559	20.6520	-21.1790	74.0679	.00	188.00
	Power Infra	43	.4651	2.0395	.3110	-.1625	1.0928	.00	12.00
	Public	149	6.7987	37.6289	3.0827	.7069	12.8904	.00	317.00
	Railways	54	3.1852	6.9691	.9484	1.2830	5.0874	.00	26.00
	Roadways	7	1.8571	3.7607	1.4214	-1.6209	5.3352	.00	10.00
	Schools	1	.0000	.	.	.	.	.00	.00
	Subways	4	3.5000	5.7446	2.8723	-5.6409	12.6409	.00	12.00
	Train St.	17	19.8235	54.2117	13.1483	-8.0495	47.6966	.00	201.00
	Vehicles	6	2.8333	4.4008	1.7966	-1.7850	7.4516	.00	9.00
	Water Treatment Facil.	10	.9000	1.6633	.5260	-.2899	2.0899	.00	5.00
	Total	1080	3.0231	29.0644	.8844	1.2878	4.7585	.00	741.00
injuries	Avaition Infra	25	3.4400	7.8373	1.5675	.2049	6.6751	.00	30.00
	Chemical Plant	9	2.4444	5.7033	1.9011	-1.9395	6.8284	.00	17.00
	Comm. Infra	5	3.2000	4.3818	1.9596	-2.2407	8.6407	.00	8.00
	Damns & Wat.	12	1.7500	2.8002	.8083	-2.914E-02	3.5291	.00	9.00
	Embass/Cons.	491	9.0061	180.5537	8.1483	-7.0038	25.0160	.00	4000.00
	Finan Inst.	121	15.5537	133.1932	12.1085	-8.4202	39.5277	.00	1440.00
	Food Stor Facil.	1	.0000	.	.	.	.	.00	.00
	Hospitals	10	9.4000	18.3073	5.7893	-3.6962	22.4962	.00	60.00
	Mil. Bases and Pol. St.	12	7.6667	15.6050	4.5048	-2.2483	17.5816	.00	50.00
	Oil/Gas	94	1.8298	11.4832	1.1844	-.5222	4.1818	.00	100.00
	Other	9	19.5556	36.2323	12.0774	-8.2950	47.4061	.00	90.00
	Power Infra	43	1.4419	5.4393	.8295	-.2321	3.1158	.00	33.00
	Public	149	26.4094	138.6058	11.3550	3.9705	48.8483	.00	1250.00
	Railways	54	11.8519	28.6984	3.9054	4.0187	19.6850	.00	150.00
	Roadways	7	3.8571	9.3350	3.5283	-4.7763	12.4906	.00	25.00
	Schools	1	5.0000	.	.	.	.	5.00	5.00
	Subways	4	284.5000	504.5404	252.2702	-518.3363	1087.3363	.00	1038.00
	Train St.	17	134.3529	432.7189	104.9497	-88.1306	356.8365	.00	1800.00
	Vehicles	6	4.8333	6.1779	2.5221	-1.6500	11.3167	.00	15.00
	Water Treatment Facil.	10	.2000	.6325	.2000	-.2524	.6524	.00	2.00
	Total	1080	13.9861	153.3913	4.6675	4.8276	23.1446	.00	4000.00
total number of casualties	Avaition Infra	25	5.6000	13.1244	2.6249	.1825	11.0175	.00	50.00
	Chemical Plant	9	4.5556	8.5894	2.8631	-2.0468	11.1580	.00	22.00
	Comm. Infra	5	4.0000	5.6569	2.5298	-3.0239	11.0239	.00	12.00
	Damns & Wat.	12	6.9167	17.8858	5.1632	-4.4474	18.2808	.00	63.00
	Embass/Cons.	491	9.6130	190.1752	8.5825	-7.2500	26.4761	.00	4213.00
	Finan Inst.	121	16.8843	141.3437	12.8494	-8.5567	42.3253	.00	1523.00
	Food Stor Facil.	1	.0000	.	.	.	.	.00	.00
	Hospitals	10	11.5000	19.9011	6.2933	-2.7364	25.7364	.00	66.00
	Mil. Bases and Pol. St.	12	9.9167	21.3476	6.1625	-3.6469	23.4803	.00	71.00
	Oil/Gas	94	10.1915	86.9432	8.9675	-7.6162	27.9992	.00	841.00
	Other	9	46.0000	87.8479	29.2826	-21.5259	113.5259	.00	264.00
	Power Infra	43	1.9070	7.3737	1.1245	-.3623	4.1763	.00	45.00
	Public	149	33.2081	166.2629	13.6208	6.2917	60.1244	.00	1567.00
	Railways	54	15.0370	33.6850	4.5839	5.8428	24.2313	.00	175.00
	Roadways	7	5.7143	12.9963	4.9122	-6.3053	17.7339	.00	35.00
	Schools	1	5.0000	.	.	.	.	5.00	5.00
	Subways	4	288.0000	510.2705	255.1353	-523.9543	1099.9543	.00	1050.00
	Train St.	17	154.1765	482.7282	117.0788	-94.0195	402.3724	.00	2001.00
	Vehicles	6	7.6667	8.5245	3.4801	-1.2792	16.6126	.00	23.00
	Water Treatment Facil.	10	1.1000	1.9120	.6046	-.2677	2.4677	.00	5.00
	Total	1080	17.0093	167.5169	5.0974	7.0074	27.0112	.00	4213.00

Test of Homogeneity of Variances

	Levene Statistic	df1	df2	Sig.
fatalities	3.534	19	1060	.000
injuries	3.063	19	1060	.000
total number of casualties	3.125	19	1060	.000

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
fatalities	Between Groups	18229.851	19	959.466	1.139	.305
	Within Groups	893244.570	1060	842.684		
	Total	911474.421	1079			
injuries	Between Groups	606108.292	19	31900.436	1.365	.135
	Within Groups	24781564	1060	23378.834		
	Total	25387673	1079			
total number of casualties	Between Groups	713513.705	19	37553.353	1.346	.145
	Within Groups	29565288	1060	27891.781		
	Total	30278802	1079			

Appendix IV: POSSIBLE MODEL EXTENSIONS*

A large number of threat assessment models were reviewed, analyzed, and taken into account during the development of the DECIDe Framework. Many of these approaches may still offer additional ways to extend and enhance the work presented in this study. (Alternatively, some of these approaches may be enhanced or extended by the DECIDe Framework.) This appendix briefly describes the key models that merit further consideration.

Name	Developer(s)	Supporting Literature	Description
An Integrated Framework for the Analysis of Group Risk for Terrorism	Jerrold M. Post, Keven G. Ruby & Eric D Shaw	Jerrold M. Post, Keven G. Ruby; and Eric D. Shaw, "The Radical Group in Context: An Integrated Framework for the Analysis of Group Risk for Terrorism," *Studies in Conflict and Terrorism* 25 (2002), p. 73-126.	"This framework provides 32 critical variables as identified by experts that can be used to assess the likelihood ("risk") that a particular group will tend toward political violence. The framework's variables are identified within 4 overarching categories. These include: 1) External factors, including historical, cultural, and contextual features; 2) Key actors affecting the group, including the regime and other opponents, as well as Constituents and Supporters; 3) The Group/Organization: Characteristics, Processes, and Structures, including an examination of such factors as leadership style and decision making, group experience with violence, and group ideology and goals; and 4) Characteristics of the /immediate Situation, including Triggering Events."
Risk Management Approach	DoD	U.S. General Accounting Office. "Combating Terrorism: Threat And Risk Assessments Can Help Prioritize and Target Program Investments". GAO/NSIAD-98-74. U.S. General Accounting Office, "Combating Terrorism: Actions Needed to Guide Services' Antiterrorism Efforts at Installations," November 2002. National Infrastructure Protection Center, "Risk Management: An Essential Guide to Protecting Critical Assets," November 2002. http://www.nipc.gov/publications/nipcpub/P-Risk%20Management.pdf	"A multidisciplinary team of experts is used to identify and evaluate threats, assets' criticality, vulnerabilities, and countermeasures to manage or reduce risk. This information is used to generate specific threat scenarios from valid intelligence and threat data that are then paired against vulnerabilities in critical assets. Weights or values are assigned to these threat-asset vulnerability pairings according to the likelihood of such events occurring and the consequences of assets being compromised or attacked." "The required assessments of threat, vulnerability and criticality of assets form the foundation of each installation's antiterrorism plan and support a risk management approach to resource allocation. These three assessments are designed to assess (1) the threats to the installation, (2) the installation's vulnerabilities, and (3) the installation's critical assets."

* This appendix was prepared by Charles Blair, Andrew Jayne and Kevin S. Moran.

			"The threat assessment identifies and evaluates potential threats on the basis of such factors as the threats' capabilities, intentions, and past activities. This assessment represents a systematic approach to identify potential threats before they materialize. However, this assessment might not adequately capture some emerging threats, even in cases where the assessment is frequently updated. The risk management approach therefore uses vulnerability and asset criticality assessments as additional inputs to the risk management decision-making process."
Wheel of Crises	Ian I. Mitroff & Murat C. Alpaslan	Ian I. Mitroff, Murat C. Alpaslan, "Preparing for Evil," Harvard Business Review, April 2003.	"Two executives think more broadly about potential crises, a wheel is spun on which a variety of categories of crises are listed. After each spin, executives are required to consider and discuss all the normal and abnormal crises of that particular kind they can imagine. The categories on the wheel are: 1) Criminal Crises such as product tampering, kidnapping or hostage taking, and acts of terrorism; 2) Information Crises such as theft of proprietary information, tampering with official records, and cyber attacks; 3) Reputation Crises such as rumors and logo tampering."
Bioterrorism Threat Assessment	Bruce Hope	Bruce K. Hope, "A Risk Assessment Perspective on Bioterrorist Threats to the U.S. Food Supply," unpublished paper.	"Hope proposes a five part assessment method to evaluate, anticipate and manage various bio-threat scenarios. The five parts include: 1) Problem Formulation- Defining the attack scenario (target and exposure mode) and target (an asset and one or more of its attributes potentially at risk, considering the bioterrorist's motivations and objectives); 2) Hazard Characterization- Estimating the probable nature and magnitude of hazard posed to that target by that bio-agent; 3) Hazard Identification- Identifying which bio-agent a bioterrorist is most likely to choose, considering the bioterrorist's deployment capabilities, the bio-agent's hazard capabilities, and the target. Inability to deploy the preferred bio-agent will require either revision of targets or upgrading of deployment capabilities; 4) Exposure Assessment- Estimating the probability of the target being exposed to the bio-agent via the exposure mode preferred by the bio-terrorist or required by the bio-agent; 5) Risk Characterization- Estimating the probability of occurrence of the desired adverse outcome in the target due to exposure to the bio-agent. In the absence of extensive empirical data, fault tree analysis (FTA) is proposed as an analytical technique appropriate for: (a) identifying and structuring risk factors and their relationships, (b) providing a preliminary

			answer to the risk question posed here, and (c) identifying data needed for an empirically more robust model."
Brief Adversary Threat Loss Estimator (BATLE)	Sandia National Laboratories (SNL)	Harry F. Martz and Mark E. Johnson, "Risk Analysis of Terrorist Attacks," *Risk Analysis* 7, (1987).	"This model is designed to be a simple, flexible, low resolution model which can be readily used to assess the security of many different kinds of systems. The model provides analytical probabilistic output of the outcome of a small-scale engagement between an adversary and security force. It uses a semi-Markov probability model to represent the engagement and considers such combatant characteristic as force size, posture, proficiency, delay tactics, weapons type, and defense or assault tactics. Site parameters include cover, illumination intensity, security reinforcements, and range of the engagement. In calculating $P(W_s)$ no security response force reinforcements are incorporated, because only the guard force is involved in the engagement. The output consists of both transient and steady state probability distributions of the surviving number of adversaries and guards."
SILENT VECTOR: Recommended Threat-Vulnerability Integration Analysis	Center for Strategic and International Studies (CSIS)	Philip Anderson, "Threat-Vulnerability Integration: A Methodology for Risk Assessment," Center for Strategic and International Studies, Washington D.C.	"The Threat-Vulnerability Integration Analysis depicts a level of risk that takes into consideration known or implied terrorist capabilities against the vulnerabilities of selected targets. Along the horizontal axis, it assumes input that results from a systematic, continuous process of analyzing terrorist intent, capabilities, tactics and the environment in which he will operate – a view from the terrorist perspective. Along the vertical axis, the methodology assumes input that results from a systematic, continuous process of analyzing the vulnerability of targets within the United States including target 'attractiveness' – again, from the terrorist perspective." "Attributes of the attack means which must be considered include: accuracy (degree of difficulty in delivering the attack means to the target); destructive capacity (payload size, weight, speed, etc); flexibility (degree of difficulty in attack coordination and presence of contingency plans); opportunity (access to the target)." "Attributes of the target that must be addressed in detail include common elements of physical security, *as viewed from the terrorist perspective*, including: size and visibility; physical construction (hardness of target, failsafe mechanisms, stand-off distances); normal safety features (inherent design, accident mitigation systems, early warning systems, security personnel awareness & training, ability to mount counter-attack); destructive capacity of the target (magnitude of damage beyond the facility); accessibility (access control, personnel screening, vehicle/freight/package inspections); target value (system criticality, attractiveness, symbolism, death toll, economic disruption/damage)."

Federal Security Risk Management (FSRM)	General Services Administration (GSA)	Nancy A. Renfroe, and Joseph L. Smith, "Threat/Vulnerability Assessments and Risk Analysis," Whole Building Design Guide, Accessed on 03/11/2004 at: http://www/wbdg/org/design/res-print.php?rp=27	"A combination of the impact of loss rating and the vulnerability rating can be used to evaluate the potential risk to the facility from a given threat."
OPSEC PROCESS	Interagency OPSEC Support Staff	Chris Hawley, Gregory G. Noll, and Michael S. Hildebrand, "Operations Security for Public Safety Agencies: Special Operations for Terrorism and Hazmat Crimes," Interagency Operations Security (OPSEC) Support Staff, Operations Security, Monograph Series.	"The OPSEC process consists of five different steps: 1) identifying critical information; 2) conducting a threat analysis; 3) performing a vulnerability analysis; 4) assessing risks; and 5) applying countermeasures." "Risk Assessment specifically weighs three basic factors based on the information that has been developed in the OPSEC process. These include: Threat-Do(es) the Adversary(s) have Intent and the Capability? What does the Threat Assessment that has been conducted tell you? Vulnerability-What type of opportunity does the Adversary have to exploit the vulnerabilities that you have identified? Impact-What would the impact on your operation be if the Adversary successfully took advantage of one of your vulnerabilities?"
And / Or Attack Tree	Bruce Schneier	Bruce Schneier, *Secrets and Lies: Digital Security in the Networked World* (Wiley Publishing, Inc., 2004).	"Attack trees provide a methodical way of describing threats against, and countermeasures protecting, a system. (…) Basically, you represent attacks against a system in a tree structure, with the goal as the root node and different ways of achieving the goal as leaf nodes. By assigning values to the nodes, you can do some basic calculations with the tree… to make statements about different attacks against the goal."
Exploratory Analysis	Paul K. Davis, James H. Bigelow, & Jimmie McEver	Paul K. Davis, James H. Bigelow, and Jimmie McEver, "Exploratory Analysis and a Case History of Multiresolution, Multiperspective Modeling," Reprinted from Proceedings of the 2002 Winter Simulation Conference, Jeffrey A. Joines, Russell R. Barton, K. Kang, and Paul A. Fishwick (editors), December 2000 and Proceedings of the SPIE, Vol.4026, 2000.	"A key to treating uncertainty well is *exploratory analysis*…The objectives of exploratory analysis include understanding the implications of uncertainty for the problem at hand and informing the choice of strategy and subsequent modifications. To do so, input uncertainties (i.e., parametric uncertainties) and structural uncertainty must be identified. Input uncertainty relates to imprecise knowledge of the model's input values. Structural uncertainty relates to questions about the form of the model itself: Does it reflect all the variables on which the real-world phenomenon purportedly described by the model depends? Is the analytical form correct? Input exploration, which can help address some of these uncertainties, involves conducting model runs across the space of cases defined by discrete values of the parameters within their plausible domains. *Probabilistic exploration* represents uncertainty about the input parameters through distribution functions representing the totality of one's so-called objective and subjective knowledge. The preferred approach treats some uncertainties parametrically and others with uncertainty distributions. That is, it is *hybrid exploration*."

ITERATE Database: Events Approach		Edward F. Mickolus, "How Do We Know We're Winning the War Against Terrorists? Issues in Measurement," *Studies in Conflict and Terrorism* 25, (2002), pp. 151-160.	"Taking an events approach, one assumes that the behaviors of terrorists are patterned, and that the discovery of these patterns through even the simplest of statistical procedures can be helpful in combating terrorism. With ITERATE, we code for circa 150 variables in the overall categories of COMMON aspects and the FATE of terrorists. We also examine variables that are common to HOSTAGE and HIJACKING incidents. We look at such things as date and location of the incident, type of attack, locations of the start and end of the incident (particularly useful in looking at hijackings), the scene of the crime, characteristics of the terrorists (who was responsible, number and nationality of the perpetrators), victim characteristics (number, type, and nationality), numbers of killed and wounded (separating out by nationality of victim, terrorists, and response forces), dollar amount of property damage and type of property damaged, and some information on logistics (was there an accident or logistic error involved in the terrorists' actions, weapons used, did the terrorists appear to succeed in their logistic aims, i.e., did the bomb go off, as opposed to did they get publicity?)."
Longitudinal Research	Charles Tilly	Robert W. White, "Issues in the Study of Political Violence: Understanding the Motives of Participants in Small Group Political Violence," *Frank Cass Journals Terrorism and Political Violence* 12, (Spring 2000), pp. 95-108.	"Longitudinal Research is a holistic approach in exploring the motives of people who engage in terrorism. Its research is in depth and accounts for the general political arena that influences, and is influenced by, such actors. The best research on small-group political violence is undertaken by researchers who, on some level, interact with the people being researched."
Predictive Analysis		Rick Whiting, "Companies Boost Sales Efforts with Predictive Analysis," Information Week, Accessed on 6/7/2002.	"Predictive analysis is a technique that models historical data with assumptive future conditions to predict outcomes or events. Predictive analysis includes forecasting and propensity analysis. Forecasting identifies trends and predicts future sales, for example. Propensity analysis uses data-mining algorithms such as regression analysis, decision trees, clustering, and neural networks to calculate predilections for certain activities."
Preference Analysis	Ralph L. Keeney & Howard Raiffa	Ralph L. Keeney and Howard Raiffa, *Decisions with Multiple Objectives: Preferences and Value Tradeoffs* (Cambridge: Cambridge University Press, 1993).	"The following approach suggests how preference aspects of analysis might be used more constructively. It involves the following major steps: PREANALYSIS. A unitary decision maker is assumed who is undecided about the course of action he or she should take in a particular problem. The problem has been identified and the viable action alternatives are given. STRUCTURAL ANALYSIS. The decision maker structures the qualitative anatomy of his problem. What choices can he make now? What choices can he defer? How can he make choices that are based on information learned along the way? What experiments can he perform? What information can he gather purposefully and what can he

			learn during the normal course of events without intentional intervention? These questions are put into an orderly package by a decision tree. UNCERTAINTY ANALYSIS: past empirical data, on assumptions fed into and results taken from various stochastic, dynamic models, on expert testimony (duly calibrated, to take into account personal idiosyncrasies and biases resulting from conflict of interest positions), and on the subjective judgments of the decision maker. The assignments should be checked for internal consistencies. The decision maker must assign numbers to consequences such that the maximization of *expected utility* becomes the appropriate criterion for the decision maker's optimal action."
Collective Action Modeler		Mark Irving Lichbach, *The Rebel's Dilemma* (Ann Arbor: University of Michigan Press, 1998), pp. ix-xiv, 50-99, and 167-77.	"As a rational dissident comes to believe that his or her contribution makes a difference in the likelihood that the primary goal (PG) will be obtained, his or her participation in collective dissent increases. A basic corollary follows: participants in collective dissent will report higher expectations of their personal efficacy than non-participants. Intensity of demand (zealotry, sect. 3.1) may therefore substitute for personal efficacy. Thus, the greater a rational dissident's intensity of demand for a PG, the smaller his or her 'probability of making a difference' needs to be before he or she participates in collective dissent. Similarly, personal efficacy may substitute for intensity of demand. Thus, more powerful dissidents (i.e., those with a greater 'probability of making a difference') require less utility differential to participate in collective dissent."
Multiple Model Approach	John Monohan et al.	John Monohan, et. al., *Rethinking Risk Assessment: The MacArthur Study of Mental Disorder and Violence* (Oxford: Oxford University Press, 2001).	"Multiple models can be combined to produce risk assessments that are much more accurate than any single risk assessment model taken alone. Crucial is grasping the concept that by combining a large number of models, each of which contains a different combination of risk factors, the stability of the risk assessments for each individual is increased dramatically. Using this "multiple model" approach, we ultimately combined the results of five prediction models generated by the Iterative Classification Tree methodology. The multiple model approach minimizes the problem of data over-fitting that can result when a single "best" prediction model is used."
Game Theory		Todd Sandler and Daniel G. Arce M., "Terrorism & Game Theory," *Simulation and Gaming* 34, (September 2003), pp. 319-337.	"Game theory is an appropriate tool for examining terrorism for a number of reasons. First, game theory captures the strategic interactions between terrorists and a targeted government, where actions are interdependent…Second, strategic interactions among rational actors, who are trying to act according to how they think their counterparts will act and react, characterize the interface between terrorists…Third, in terrorist situations, each side issues threats and promises to gain a strategic advantage. Fourth, terrorists and

			governments abide by the underlying rationality assumption of game theory, where a player maximizes a goal subject to constraints. Empirical support for terrorists' rationality is given credence by their predictable responses to changes in their constraints…Fifth, game-theoretic notions of bargaining are applicable to hostage negotiations and terrorist campaign-induced negotiations over demands. Sixth, uncertainty and learning in a strategic environment are relevant to all aspects of terrorism, in which the terrorists or government or both are not completely informed."
Qualitative Adversary Intent Criteria	DOE	Department of Energy, "Energy Infrastructure Vulnerability and Risk Assessment Checklists for State Governments," December 4, 2001. http://www.appanet.org/operations/checklist.pdf	"To identify and evaluate the threat environment to which an organization may be exposed the following questions should be answered: What are the specific goals and objectives of the adversary? What does the adversary gain by achieving these goals? How will the adversary achieve its goals through exploiting our assets? Is the adversary aware that the asset exists? Does the adversary know enough about the asset to plan an attack? Is the adversary willing to risk being caught? Are there other, less risky means for an adversary to attain his/her goals? What is the probability that the adversary will choose one method of attack over another? What specific events might provoke the adversary to act? What might the adversary lose in attempting to exploit our assets? Would that loss be a rational trade-off, from the adversary's perspective? To what degree is the adversary motivated?"
Individual Threat Assessment	US Secret Service	Randy Borum, Robert Fein, BryanVossekuil, and John Berglund, "Threat Assessment: Defining an Approach for Evaluating Risk of Targeted Violence," *Behavioral Sciences and the Law* 17, (1999), pp. 323-337.	"Threat assessment is a set of investigative and operational activities designed to identify, assess, and manage persons who may pose a threat of violence to identifiable targets. Conceptually, this approach is innovative in two ways: (1) it does not rely on descriptive, demographic, or psychological profiles and (2) it does not rely on verbal or written threats as a threshold for risk. Instead of looking at demographic and psychological characteristics, the threat assessment approach focuses on a subject's thinking and behaviors as a means to assess his/her progress on a pathway to violent action. The question in a threat assessment is not `What does the subject `look like'?' but 'Has the subject engaged in recent behavior that suggests that he/she is moving on a path toward violence directed toward a particular target(s)?' To accurately conduct such a threat assessment, three types of information about the subject are typically collected; identifying information, background information, and information about the subject's current situation and circumstances."
Order Theory	Jonathan David Farley	Jonathan David Farley, "Breaking Al Qaeda Cells: A Mathematical Analysis of Counterterrorism Operations (A Guide for Risk Assessment and Decision Making), *Studies in Conflict & Terrorism* 26, (2003), pp. 399–411.	"*Order theory* provides a framework for not only breaking up terrorist networks into disconnected (non-communicating) parts, but also cutting the leaders off from the followers. One criterion might be to say that a terrorist cell has been broken if it is no longer able to pass orders down

			from the leaders to the foot soldiers—the men and women who, presumably, will carry out the attacks. This is by no means the only possible criterion, but it enables us to make precise estimates of the possibility that our operations have successfully disabled a terrorist cell." "How can law enforcement *quantify* how effective it has been in disrupting a particular terrorist cell? As we have stated, one way to make this precise is to say that a terrorist cell has been disrupted *not* when all of its members have been captured or killed (which might be too costly in terms of money, agents, and agents' time), but when all chains of command have been broken. That is, the collection of nodes in the network corresponding to the terrorists who have been killed or captured should be acutest. This enables us to *calculate*—not merely guess—the probability that a terrorist cell has been disrupted."
Markov Chain	Gordon Woo	Dr. Gordon Woo, "The evolution of Terrorism Risk Modeling," Risk Management Solutions. http://www.rms.com/Publications/EvolutionTerRiskMod_Woo_JournalRe.pdf	"A Markov chain is defined by the series of states that Al Qaeda occupies, and makes transitions to and from. This is a controlled Markov chain because, whatever state Al Qaeda occupies, the police and security forces counter the prevailing threat with actions which aim ton control terrorism... In mathematical terms, these counter-actions are termed the *Markov feedback policy*."
Pre-Incident Attack Observables	Joshua Sinai	Dr. Joshua Sinai, "ICT Conference: Expert on Value, Methods of Forecasting Terrorist Incidents," FBIS Report, Document ID: GMG20031202000085, September 9, 2003.	"This model creates pre-incident attack observables during the crucial incubation period that can be identified, monitored, preempted, and disrupted at the earliest possible phases. The pre-incident incubation process can be broken into four phases: the formation of a group; planning an attack; developing a capability; and executing the operation. This model uses 31 indicator categories to enable the user to understand all the indicators that need to be looked at in figuring out the warfare proclivity of a terrorist group."
Game Theory which Incorporates Ideology	Gordon Woo	Dr. Gordon Woo, "Mathematical Aspects of Terrorism Hazard", Risk Management Solutions. http://www.rms.com/Publications/MathematicalAspectsOfTerrorHaz_Woo.asp Dr. Gordon Woo, "Understanding Terrorism Risk," Risk Management Solutions, http://www.rms.com/Publications/UnderstandTerRisk_Woo_RiskReport04.pdf	"Game theory predicts that, as prime targets are hardened, rational terrorists will tend to substitute lesser softer targets…Target substitution, as this is called, is a prediction about the rational behavior of terrorists, affirmation of which must ultimately come from the mouths of terrorists themselves." "If paradise is the payoff for martyrdom, then an Islamic militant would wish to be maximally sure of hitting the target, and would tend to attack later (i.e. closer to the target). Taking sufficient time to achieve mission success is a trait of al-Qaeda. The patience and diligence with which al-Qaeda operations are planned to reflect underlying fundamentalist belief in the high payoff of a suicide mission. Not just the preparation time, but also the swarm attack is a feature of al-Qaeda strategy which is comprehensible in game theory terms."

			"In applying game theory to terrorism, it is important to leave behind popular notions of rationality, and to return to the formal mathematical definition of rational behavior, namely that actions are taken in accordance with a specific preference relation. There is no requirement that a terrorist's preference relation should involve economic advantage or financial gain…Nor is it necessary that a terrorist's preference relation conform with those of society at large."
Microbiological Risk Assessment		Codex Alimentarius Commission, "Principles and Guidelines for the Conduct of Microbiological Risk Assessment," CAC/GL-30, 1999.	"There are seven steps to follow in conducting a Microbiological Risk Assessment: 1) Statement of Purpose of Risk Assessment; 2) Hazard Identification; 3) Exposure Assessment; 4) Hazard Characterization; 5) Risk Characterization; 6) Documentation; 7) Reassessment." The conduct of a Microbiological Risk Assessment should be transparent. Any constraints that impact on the Risk Assessment such as cost, resources or time, should be identified and their possible consequences described. The Risk Estimate should contain a description of uncertainty and where the uncertainty arose during the Risk Assessment process. Data should be such that uncertainty in the Risk Estimate can be determined; data and data collection systems should, as far as possible, be of sufficient quality and precision that uncertainty in the Risk Estimate is minimized. Wherever possible, Risk Estimates should be reassessed over time by comparison with independent data. A Microbiological Risk Assessment may need reevaluation, as new relevant information becomes available."
Natural Catastrophe Models		Bianca Markram, "An insoluble problem?," *Reactions* 24, July 2002. www.reactionsnet.com	
Law of Energy Conservation and Game Theory	Gordon Woo	Dr. Gordon Woo, "Quantitative Terrorism Risk Assessment," Risk Management Solutions, http://www.rms.com/NewsPress/Quantitative_Terrorism_Risk_Assessment.pdf	"In hydrology, the principle of minimum energy expenditure governs the pattern of river drainage networks. In a similar way to the flow of water, the flow of al-Qaeda terrorism activity is towards weapon modes and targets, against which the technical, logistical and security barriers to mission success are least. In order to express target prioritization in a quantitative way, the ranking by city and target type has to be converted into mathematical form. This interpolation is simply achieved by invoking Fechner's Law, which states that an arithmetic progression in perceptions requires a geometrical progression in their stimuli. In order to arrive at a target probability distribution, a mathematical expression needs to be obtained for the functional dependence of target probability on utility. For this, game theory is required."
Vulnerability Assessment Methodologies	Office of Domestic Preparedness, DHS	U.S. Department of Homeland Security: Office for Domestic Preparedness (OPD), "Vulnerability Assessment Methodologies Report," Phase I Final Report, July 2003.	"Risk [R] = Consequences [C] times Likelihood [L] or C x L. Likelihood can be further defined in terms of a specific vulnerability [V] that is exploited by a specific adversary or threat [T]. Each of these events is a probability. Hence, Likelihood is a conditional probability expressed as:

			[L] = p[T] x p[V]." "Risk may be defined more fully as the product of consequences or impact [I] to the owner in case of loss or damage to a valued asset, and the likelihood that the asset may be damaged or destroyed by a particular adversary exploiting a specific vulnerability: R = I x p[T] x p[V]." "The threat is any indication, circumstance, or event with the potential to cause loss of or damage to an asset. In its traditional definition, a threat is a product of intention and capability of an adversary, both manmade and natural, to undertake an action which would be detrimental to an asset. A vulnerability is a weakness that can be exploited by an adversary to gain access to an asset."
Game Theory and Approximate Reasoning	Los Alamos National Laboratory (LANL)	Steve Eisenhower, Terry Bott, and D.V. Rao, "Assessing the Risk of Nuclear Terrorism Using Logic Evolved Decision Analysis," Los Alamos National Laboratory (LA-UR-03-3467).	"The model proposed here is based on a game theoretic perspective where the set of attackers and the defender play an extensive game with imperfect information. We perform the risk evaluation using approximate reasoning (AR). AR uses a series of forward-chained rule bases to emulate expert judgment. It is particularly well suited to decision problems where much of the data is qualitative and many of the relevant factors and their importance are perceptual in nature." "Two process trees are essential for decision analysis: a *possibility* tree that represents a comprehensive set of alternatives, in this case terrorist attack scenarios and an *inference* tree that defines how a metric is to be inferred." "The inferential model incorporates a game theoretic perspective. The game to be played is asymmetric. A specific attacker will choose to attempt only a particular subset of attack scenarios associated with particular targets and employing specific attack modes. He will attempt to allocate his assets in order to inflict the maximum amount of terror. The defender on the other hand must try to protect all of the targets for which he bears responsibility against all attack scenarios. He will attempt to minimize his risk." "The model is advanced because it is insufficient to concentrate on the vulnerability of homeland targets to the exclusion of attacker motivation, intentions and capability."
Logic Evolved Decision-Making (LED)	Los Alamos National Laboratory (LANL)	Terr F. Bott and Stephen Eisenhower, "Evaluating Complex Systems When Numerical Information is Sparse," Los Alamos National Laboratory. Terry F. Bott, Stephen W. Eisenhower, Jonathan Kingson, and Brian P. Key, "A New Graphical Tool for Building Logic-Gate Trees," Los Alamos National Laboratory and Innovative Technical Solutions, Inc.	"A system behavior of interest is modeled with a deductive logic model called a system process tree, which gives us an organized list of possible paths leading to the final system state of interest. A forward-chaining implication structure that combines individual factors using approximate reasoning (AR) techniques produces a Figure of Merit

			evaluation of each of the possible paths to a system state. The method for evaluating the possibilities can then be described as a forward-linked implication structure." "The basic elements of a decision model are: 1) Determine the possibilities or alternatives; 2) Select the metric to rank the possibilities; 3) Design an inferential model for the metric; 4) Rank the possibilities according to the metric; 5) Express the degree of uncertainty in the results; 6) Express the results in a form useful to the decision maker." "The fundamental assumption underlying the use of the possibility tree is that complex system behavior can be modeled by logically connecting sets of discrete events and states, called the "elements" of the tree. This fundamental assumption is rendered less restrictive by introducing logic gates that model complex relationships between elements such as cycles and conditional branching." "To construct a possibility tree, information about system processes is extracted from sources of general knowledge, expert judgments, and observations, by analogy, or through heuristics. This knowledge is converted into discrete elements that are linked together using logic gates as connectives. The system characteristics thus are uncovered deductively from all known sources of relevant information using step-by-step causality-based reasoning. This reasoning process produces a hierarchical tree structure with well-defined connections between levels of the tree. The tree structure often can be used to capture competing views about the possible causes for various events in a single-tree structure."
Cognitive Manager Model		Karen Guttieri, Michael D. Wallace, Peter Suedfeld, University of British Columbia, "The Integrative Complexity of American Decision Makers in the Cuban Missile Crisis," *Journal of Conflict Resolution* 39, No. 4, (Beverly Hills: Sage Publications, Inc., 1995).	"The policy-maker considers a number of dimensions of the problem or perspectives on it and searches for alternative solutions (i.e., differentiation), weighs the alternatives in light of their probabilities of success, and chooses a course of action designed to maximize positive values and minimize losses, based on theoretical beliefs about the effects of those actions and other considerations such as morality, tradition, and values (i.e., integration)." The cognitive manager model…portrays cognitive reaction to such stressors as analogous to the general adaptation syndrome…The mobilization of cognitive resources in response to the recognition of a crisis is analogous to the alarm reaction. Resistance, an ongoing level of relatively high complexity (depending on the perceived importance of the problem compared to other, concurrent demands), prevails."
Contributing Factor Diagram		Glenn Koller, *Risk Modeling for Determining Value and Decision Making* (Boca Raton, FL: Chapman & Hall/CRC, 2000).	"The CFD is an outgrowth of the "influence diagram." It is particularly useful for outlining work processes and to delineate logical and

			mathematical relationships between risk-model variables. It is important to recognize that a CFD is not a flow chart, particularly in that its factors are not arranged in any time- or sequence-dependent manner."
Bayesian Analysis		Glenn Koller, *Risk Modeling for Determining Value and Decision Making* (Boca Raton, FL: Chapman & Hall/CRC, 2000).	"Bayesian Model Averaging is a technique designed to help account for the uncertainty inherent in the model selection process, something which traditional statistical analysis often neglects. By averaging over many different competing models, BMA incorporates model uncertainty into conclusions about parameters and prediction. BMA has been applied successfully to many statistical model classes including linear regression, generalized linear models, Cox regression models, and discrete graphical models, in all cases improving predictive performance."
Probabilistic Branching Model		Glenn Koller, *Risk Modeling for Determining Value and Decision Making* (Boca Raton, FL: Chapman & Hall/CRC, 2000).	"Solving decision trees probabilistically simply replaces the leaf-node deterministic values with distributions, and the tree is solved many times. On each solution of the tree, a random grab is made from each leaf-node distribution and the expected value is calculated in the usual way. Repeated random grabs and solutions of the tree result in a distribution of expected values."
Monte Carlo Analysis		Glenn Koller, *Risk Modeling for Determining Value and Decision Making* (Boca Raton, FL: Chapman & Hall/CRC, 2000).	"Monte Carlo analysis uses the process of simulation to achieve a range of solutions to a problem. The technique is generally used to solve problems for which the definition of specific solution equations to calculate a specific answer is either too complex or too cumbersome to be practical. The term can be applied to any procedure that uses distribution-based random sampling to approximate solutions to probabilistic or deterministic problems. The most common application involves determining the probability that a certain event (or result) will occur and predicting the magnitude of the event."
Time Series Analysis		Glenn Koller, *Risk Modeling for Determining Value and Decision Making* (Boca Raton, FL: Chapman & Hall/CRC, 2000).	"Time-series analysis is a function that helps risk modelers better emulate actual situations, because it allows such analysis to break free of the single period assessment and to project the analysis through time. This can be done by transforming single values into previously identified distributions or by establish one or more expansion distributions."
Sensitivity Analysis		Glenn Koller, *Risk Modeling for Determining Value and Decision Making* (Boca Raton, FL: Chapman & Hall/CRC, 2000).	"Sensitivity analysis aids in identifying the elements of a risk model that were most and least important to the calculation of the answer. Most comprehensive risk studies are composed of many input and output variables. Sensitivity analysis is used to determine which risk-model input parameters contribute most to the relative outcomes of various measured scenarios."
Relative Risk Model		Glenn Koller, *Risk Modeling for Determining Value and Decision Making* (Boca Raton, FL: Chapman & Hall/CRC, 2000).	"Model used to relatively rank and compare contenders concerning particularly risk. It is designed from consensus by experts and is

			generic in nature. The benefit of such an approach is that the model can be used time and again to evaluate new or reevaluate previously considered situations. Weights are used in the model to afford those applying the risk model the ability to emphasize or de-emphasize the various model components. To communicate risk model results to decision makers, a comprehensive cost model might be developed that translates the risk mitigation actions into financial terms."