LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

UCRL-SR-208717

Assessing Terrorist Motivations for Attacking Critical "Chemical" Infrastructure

G. Ackerman, J. Bale, K. Moran

December 20, 2004

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.

Assessing Terrorist Motivations for Attacking Critical "Chemical" 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

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-SR-208717

Sponsor

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

Funding

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

Cover: A 1995 attack on the Petrokemica fertilizer plant in Kutina, Croatia by Serbian forces.

"[I]ndividuals have indeed attempted to use chemical releases from individual facilities as makeshift WMD both domestically and abroad. Some of these events have involved countries or factions hostile to the United Sates."

The U.S. 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, p. 24.

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 Investigators*:**
Charles P. Blair, Research Associate, WMDTRP
Kevin S. Moran, Research Associate, WMDTRP

***Investigators*:**
Praveen Abhayaratne, Research Associate, WMDTRP
Gary Ackerman, Director, WMDTRP
Jeff Bale, PhD, Senior Research Associate, WMDTRP
Andrew Jayne, Graduate Research Assistant, WMDTRP
Margaret Kosal, PhD, Post Doctoral Fellow, CBWNP

***Support Staff*:**
Joel Baker, Graduate Research Assistant, WMDTRP
Lydia Hansell, Graduate Research Assistant, WMDTRP
Lauren Harrison, Graduate Research Assistant, WMDTRP
Keeli Sorensen, Graduate Research Assistant, WMDTRP

TABLE OF CONTENTS

BOXES, FIGURES AND TABLES REFERENCED IN REPORT

Boxes

Figures

Tables

EXECUTIVE SUMMARY

"Individuals have indeed attempted to use chemical releases from individual facilities as makeshift WMD both domestically and abroad. Some of these events have involved countries or factions hostile to the United States."

U.S. Department of Justice, 2000[1]

Project Overview

Certain types of infrastructure – critical infrastructure (CI) – play vital roles in underpinning our economy, security, and way of life. One particular type of CI – that relating to chemicals – constitutes both an important element of our nation's infrastructure and a particularly attractive set of potential targets. This is primarily because of the large quantities of toxic industrial chemicals (TICs) it employs in various operations and because of the essential economic functions it serves.

This study attempts to minimize some of the ambiguities that presently impede chemical infrastructure threat assessments by providing new insight into the key motivational factors that affect terrorist organizations' propensity to attack chemical facilities. Prepared as a companion piece to the Center for Nonproliferation Studies' August 2004 study – "Assessing Terrorist Motivations for Attacking Critical Infrastructure" – it investigates three overarching research questions: 1) why do terrorists choose to attack chemical-related infrastructure over other targets; 2) what specific factors influence their target selection decisions concerning chemical facilities; and 3) which, if any, types of groups are most inclined to attack chemical infrastructure targets?

The study involved a multi-pronged research design, which made use of four discrete investigative techniques to answer the above questions as comprehensively as possible. These include:

- *a review of terrorism and threat assessment literature* to glean expert consensus regarding terrorist interest in targeting chemical facilities;
- *the preparation of case studies* to help identify internal group factors and contextual influences that have played a significant role in leading some terrorist groups to attack chemical facilities;
- *an examination of data from the Critical Infrastructure Terrorist Incident Catalog (CrITIC)* to further illuminate the nature of terrorist attacks against chemical facilities to date; and
- *the refinement of the DECIDe – the Determinants Effecting Critical Infrastructure Decisions – analytical framework* to make the factors and dynamics identified by the study more "usable" in future efforts to assess terrorist intentions to target chemical-related infrastructure.

[1] US 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, p 24.

Defining the Issue

Given the current lack of a clear, standard definition for what is meant by critical infrastructure relating to the chemical industry in contemporary policy discussions, CNS crafted the following one to guide its research:

> **Critical chemical infrastructure consists of those physical facilities that either: 1) the chemical industry – as defined by the NAICS – depends on to provide minimum essential levels of services and products; or 2) contain chemicals in sufficient quantities that if successfully attacked could significantly jeopardize public health and safety in surrounding communities.**

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 "chemical" critical infrastructure that have been raised in the context of policy discussions relating to terrorism to date, namely:

- *"chemical" critical infrastructure involves assets that may be found both within and outside the traditionally defined chemical industry* – to minimize the semantic confusion and ambiguity that, as discussed earlier, can be associated with the terms "chemical industry critical infrastructure" and "chemical industry and hazardous materials critical infrastructure," CNS deliberately refers to critical infrastructure related to the chemical industry and large quantities of toxic industrial chemicals as "critical chemical infrastructure;"

- *critical chemical infrastructure is significant for economic and safety reasons* – we depend on critical chemical infrastructure to maintain our economy and way of life; we also depend on such infrastructure for the safe management and appropriate use of chemicals that are often extremely toxic and/or volatile;

- *critical chemical infrastructure involves more than chemical manufacturing plants* – critical chemical infrastructure involves numerous types of assets, including but not limited to: corporate headquarters, manufacturing and processing plants, specialized transportation vehicles (such as rail tank cars, tank trucks, pipelines, and barges and ships), and storage facilities.

Literature Assessment

To establish a theoretical foundation for studying terrorist motivations for attacking critical chemical infrastructure, CNS reviewed a wide body of terrorism-related, threat assessment-focused, and industry-specific literature. A very small amount of this literature – primarily consisting of government reports, chemical industry analyses, studies by environmental organizations, and news exposés – specifically addresses the threat of terrorist attacks on chemical facilities. Most of these materials were produced after 9/11 and focus on either the possible effects of a successful terrorist attack against a chemical facility or the existing security vulnerabilities of chemical facilities. Although virtually none of this material examines terrorist motivations for attacking chemical facilities in any depth, the discussions found in these documents do provide important insight into how the issue of critical chemical infrastructure might best be understood in the context of contemporary terrorism. The literature, for example, indicates: 1) the existing reality of terrorist interest in attacking chemical facilities; and 2) the wide range of objectives terrorists might have for attacking critical chemical infrastructure.

In particular, the literature assessment highlights the fact that most analyses to date have insufficiently identified the wide range of rationales terrorists might have for targeting critical chemical infrastructure. This report argues that terrorists might target chemical infrastructure to accomplish operational objectives that fall into one or more of nine discrete categories. These include:

- causing human casualties;
- causing physical destruction;
- causing environmental contamination;
- damaging the economy;
- disrupting strategic industrial functions;
- acquiring supplies of chemicals (for later use as weapons);
- influencing the general public;
- establishing bargaining leverage for negotiations; and
- facilitating organization building efforts.

Recognizing these objectives as distinct from one another can help analysts and decision-makers remain aware of the wide range of rational, functionally-driven motivations that terrorists can have for attacking critical chemical infrastructure.

The literature assessment emphasizes three additional aspects of critical chemical infrastructure that might make it a particularly attractive target for terrorists. First, because certain chemical facilities have the potential of being damaged in ways that cause catastrophic damage, terrorists desiring the capabilities of WMD can sidestep many of the technical and resource hurdles associated with acquiring such weapons by attacking certain chemical CI. Second, chemical facilities are ubiquitous and often located near population centers and critical transportation hubs. This geographical reality offers terrorists many potential targets to choose from and numerous targets that can have cascading effects if successfully attacked. Third, most critical chemical infrastructure remains relatively – as compared to other high value targets – ill secured. Despite recognition that chemical facilities can be attacked with catastrophic consequences, little has been done to enhance physical security around most chemical facilities. As a consequence, they remain a particularly vulnerable target set.

CrITIC

CrITIC – the Critical Infrastructure Terrorist Incident Catalog – is a database 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. The database enables the examination of historic trends of critical infrastructure attacks conducted by terrorists.

As used in this study, CrITIC highlights the extremely low incident of terrorist attacks against chemical infrastructure targets to date. (See Table ES-1.) While the small number of terrorist-initiated attacks on chemical facilities is heartening, this situation makes discerning motivational patterns and formulating conclusions problematic. The few cases that were identified suggest that the primary motivation behind chemical infrastructure attacks thus far has been group opposition to ruling governments. If one extrapolates narrowly, which may well be misleading, the historical record suggests that the most likely scenario for a terrorist attack on a domestic U.S. chemical facility would be carried out by domestic U.S. terrorists. As discussed in the literature assessment section, however, recent information related to al Qa`ida and several other groups indicates that this "trend" may be changing.

Little can be deduced from the cases concerning capabilities required by terrorists to attack. To do significant damage that truly impacts the U.S. critical infrastructure – rather than inflicting symbolic damage or causing large numbers of casualties – would require the large-scale targeting of select facilities, especially those that are key manufacturers of critical chemicals or single producers of raw chemicals. Most potentially catastrophic for the U.S. chemical critical infrastructure would be a coordinated attack on a number of facilities responsible for key precursors, the disruption of which would cause a bottleneck blockage. Fortunately, the selection of such facilities would require sophisticated knowledge of chemical manufacturers, industrial processes, distribution, and warehousing. It would also require a substantial effort by a relatively large, well-financed terrorist group with access to individuals with specific scientific or technical knowledge. That said, some of the incidents analyzed demonstrate that damage at even solitary plants can yield significant human and economic consequences, and that high levels of technical expertise are not necessarily required to cause major accidents.

Finally, if the historical record is indicative of future terrorist attacks then the number one priority should be increasing basic perimeter security in order to prevent a bomb or other incendiary device from harming a facility. The structural integrity of storage tanks and other vessels containing large volumes of flammable materials should be reinforced wherever possible.

DECIDe Framework

This study was undertaken to develop a greater understanding of the factors and dynamics that induce terrorists to attack critical chemical 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 such 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 chemical facilities.

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 other areas of 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.

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.

Perpetrators / Year	Motivation/Objective	Ideology	Target / Location	Tactic	Delivery	Outcome
MLN/Tupamaros (1965)	Demonstrate anti-US sentiment	Leftist	Bayer A.G. Facility Uruguay	Bomb	Unknown	None specified
People's Resistance Army (1974)	Protest U.S. support of Greek government	Leftist	Dow Plastics Plant Lavrion, Greece.	5 Bombs	Planted in facility	Two killed; unknown number of injuries
Shining Path (1983)	Anti-government; anti-US sentiment	Leftist	Bayer A.G. Plastics Plant Lima, Peru	Bombs	Planted in facility	$30 million in property damages; no specific number of fatalities or casualties
Unknown (1984)	Probable Accident / Possible Sabotage	Unknown	Union Carb Pesticide Plant Bhopal, India	Gas Leak	NA	Thousands of deaths and injuries
Peace Conquerors (1985)	Protest corporate environmental practices and policies; anti-US sentiment	Eco-Radical	Bayer A.G. Brussels HQ Brussels, Belgium	Bomb	Placed in a mailbox adjacent to Bayer headquarters	Property damage
Peace Conquerors (1985)	Revenge for 1984 Bhopal accident; protest military policies	Eco-Radical	Union Carb. Battery Plant Rosebury, Australia	Bomb	Placed in facility	Property damage
Red Army Faction – Suspected (1986)	Unknown	Leftist	Bayer A.G. Chemical Plant Cologne, West Germany	2 Bombs	Unknown	None specified
Red Army Faction – Suspected (1989)	Unknown	Leftist	Bayer Research Center Düsseldorf, West Germany	Bomb	Unknown	Bombs deactivated before exploding
Middle Eastern Islamic Liberation Front (ILF) – Claim Only (1990)	Probable Accident / ILF claim: to protest US support of Israel; hinder US defense production	Anti-American / Anti-Israeli	ARCO MTBE Facility Channelview, Texas	Explosion	NA	Widespread property damage; seventeen deaths and five injuries; explosion due to accident, not terrorism
Unknown (2004)	Anti-American; anti-West	Religious (Islamist)	ABB Lummas Global Inc (Representative Target) Saudi Arabia	Firearms	Gunmen	U.S. ambassador to Saudi Arabia urging Americans to "Go home. We cannot protect you"

Table ES-1: Summary of CrITIC Chemical Infrastructure Attacks

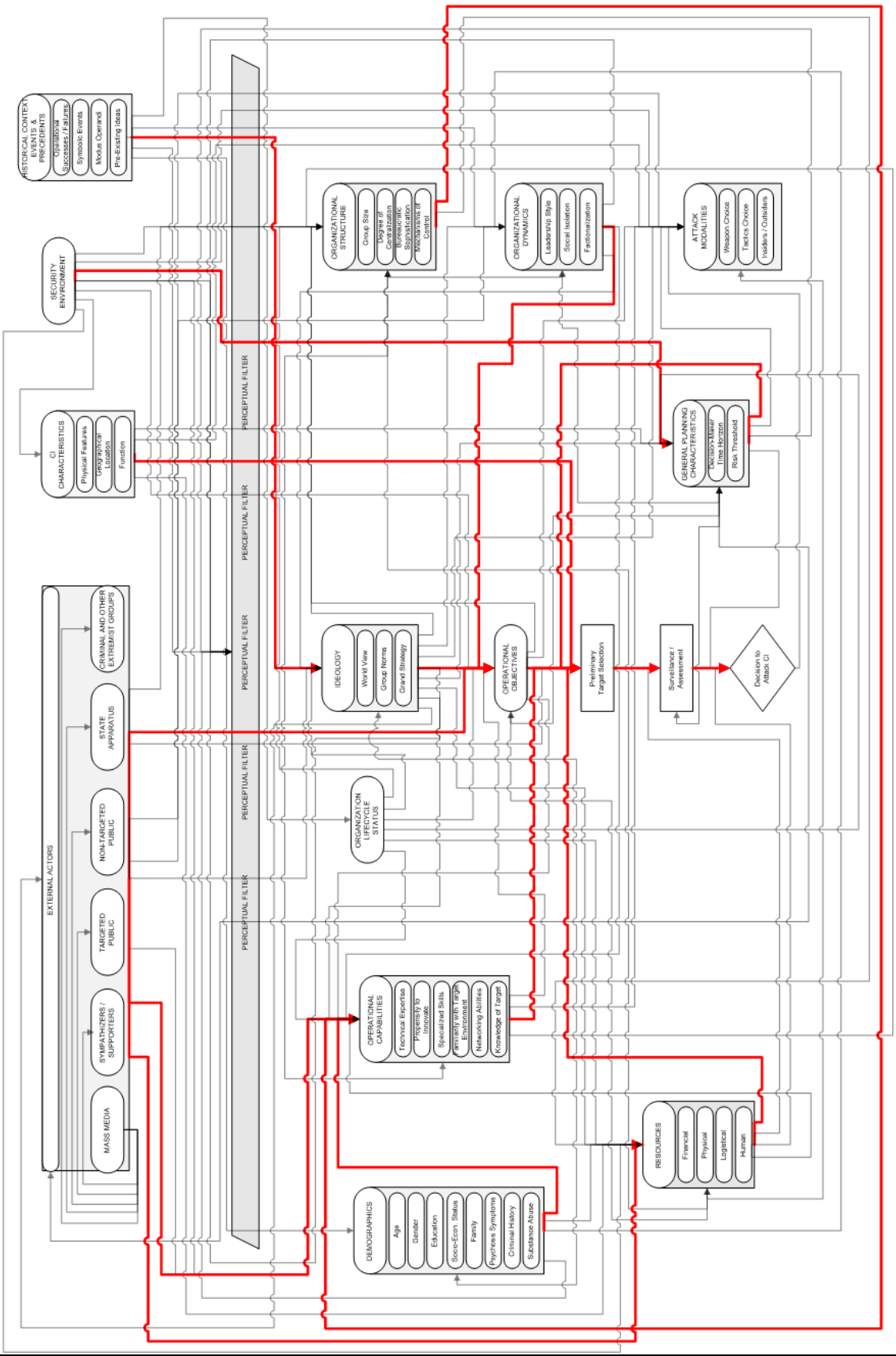


Figure ES-1: Contributing Factors Diagram

Section 1

INTRODUCTION

A. Study 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 also well 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.

There is widespread agreement within the government, private sector, and research communities that chemical facilities, in particular, constitute both an important element of our nation's infrastructure and a particularly attractive set of potential targets. This is primarily because of the large quantities of toxic industrial chemicals (TICs) they employ in their operations and because of the essential economic functions many serve. There is less agreement, however, as to how immediate or how significant the risk of terrorist attacks on such facilities may be. A 2004 report prepared for Congress attributes the difficulty in assessing these risks to three general causes: "there are few prior examples of terrorists targeting chemical facilities; numerous factors theoretically may increase or decrease such risks; and interactions among factors influencing risks are dynamic and changing."[2]

This study attempts to minimize some of the ambiguities that presently impede chemical infrastructure threat assessments by providing new insight into the key motivational factors that affect terrorist organizations' propensity to attack chemical facilities. Specifically, it builds on the analysis begun in the Center for Nonproliferation Studies' August 2004 study – "Assessing Terrorist Motivations for Attacking Critical Infrastructure" – and investigates three overarching research questions: 1) why do terrorists choose to attack chemical-related infrastructure over other targets; 2) what specific factors influence their target selection decisions concerning chemical facilities; and 3) which, if any, types of groups are most inclined to attack chemical infrastructure targets?

B. Methodological Overview

Prepared as a companion piece to CNS' August 2004 terrorism and critical infrastructure (CI) report, this study is firmly grounded in the findings and approach of the earlier project. In particular, it employs the same multi-pronged research design used to investigate terrorist target selection processes as was used in the initial study. Specifically, it makes use of four discrete investigative techniques to answer the above questions as comprehensively as possible. These include:

- *a review of terrorism and threat assessment literature* to glean expert consensus regarding terrorist interest in targeting chemical facilities;

[2] Linda-Jo Schierow, "Chemical Plant Security," Congressional Research Service, January 20, 2004, p. 5.

- *the preparation of case studies* to help identify internal group factors and contextual influences that have played a significant role in leading some terrorist groups to attack chemical facilities;

- *an examination of data from the Critical Infrastructure Terrorist Incident Catalog (CrITIC)* to further illuminate the nature of terrorist attacks against chemical facilities to date; and

- *the refinement of the DECIDe – the Determinants Effecting Critical Infrastructure Decisions – analytical framework* to make the factors and dynamics identified by the study more "usable" in future efforts to assess terrorist intentions to target chemical-related infrastructure.

Because this document is intended to be read in conjunction with CNS' earlier study on terrorism and CI, it deliberately minimizes the presentation of material and findings addressed in the August 2004 report. For reference purposes, adapted versions of the original report's discussion of terminology and its executive summary are included in Appendices I and II, respectively.

C. Defining Critical "Chemical" Infrastructure

The Threat Assessment Context

Given that this study of chemical related critical infrastructure is grounded in the context of terrorism threat assessment, it is appropriate to begin with a review of the general nature of threat assessment.[3] Technically speaking, the term is a sub-category of "risk assessment," which deals with the two main hazard mitigation issues of chance and consequence. Chance refers to the likelihood that an undesirable incident will take place. Consequence refers to the expected results of such an event.[4] The term "threat assessment"[5] falls within the former category, while consequence management is part of the latter.

Threat assessment is typically the first step in risk assessment efforts and involves four broad interrelated activities: 1) identifying and defining the specific asset (or class of assets) to be assessed; 2) quantifying the asset's value; 3) determining the asset's vulnerability to attack; and 4) evaluating the likelihood that the asset will be attacked. This particular study is concerned with the last activity – determining likelihood of attack – in which analysts seek to determine who potential attackers might be, how likely they are to attack the asset, and how capable they might be of succeeding in an attack. The answers to these questions depend significantly on both the terrorists' *perception* of the asset's (the potential target's) value and vulnerability, and their own capability to exploit such weaknesses. To attackers, the calculus used to determine a target's value is often a subjective understanding of the target's symbolic value, the expected impact (in economic, functional, human and political terms) that damage or destruction of the target is likely to produce, and the psychological impact an attack on the asset would have on prospective target audiences. Similarly, attackers assess target vulnerability largely as a function of the target's perceived defenses in relation to their own perceived capabilities.

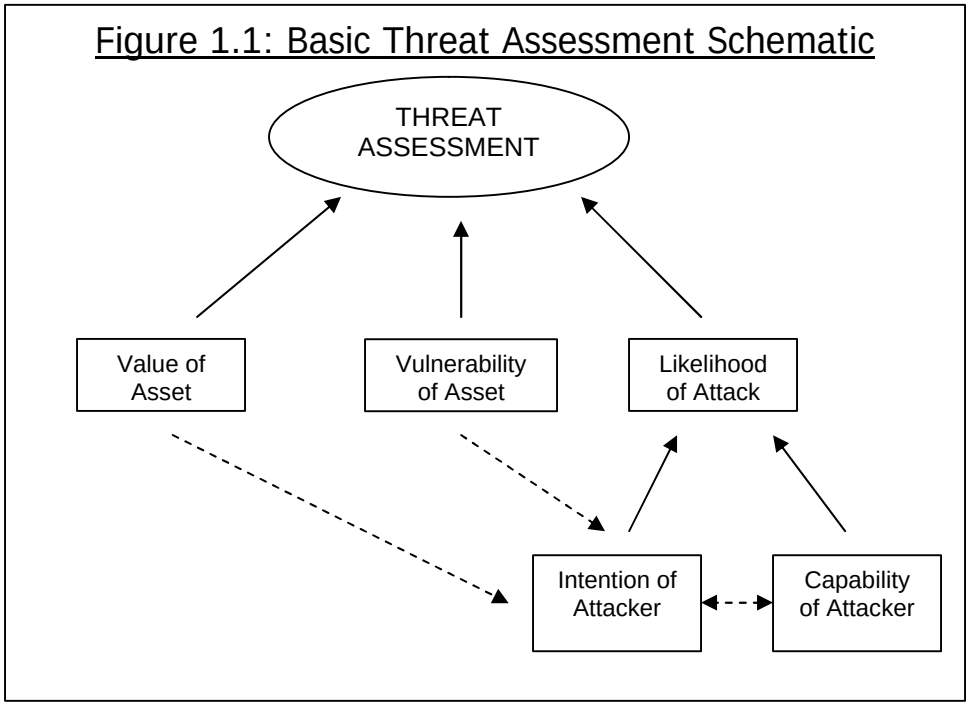
---

[3] A more detailed discussion of this concept may be found in Chapter One (pages 1-3) of CNS' "Assessing Terrorist Motivations for Attacking Critical Infrastructure."

[4] "Consequence management," is not a focus of the current study.

[5] Aanalysis 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.* <http://www/wbdg/org/design/res-print.php?rp=27>). The current study therefore defines these as it uses them.

Figure 1.1 illustrates this dynamic, with dotted lines representing the attacker's perception.



Determining the likelihood of an attack is best undertaken after the "objective" value and vulnerability of the asset have been established, and after the attackers' "subjective" target assessments have been estimated. Sadly, most open-source threat analyses deal with the "likelihood" aspect of this process 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. The reasons for this, no doubt, include the fact that the motivational aspects of threat assessment are exogenous and highly subjective factors which are often difficult to quantify.

The importance of including the motivations of potential attackers in the calculus of risk analysis cannot be emphasized enough. Neglecting the motivational aspects of threat assessment can result in sub-optimal outcomes, especially in the forms of inordinate focus on worst-case terrorism scenarios and misevaluations of threats posed to potential targets. 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 specific 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 the well-known political scientist Robert Jervis once noted, "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 broadens existing understanding.

[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.

The "Critical Infrastructure" Context

To best evaluate these issues as related to critical chemical infrastructure, it is first essential to understand the concept "critical infrastructure."[7] As noted in CNS' initial terrorism and CI study, the term critical infrastructure has generated numerous perspectives and opinions, but few standard or agreed-upon definitions. It is a fluid concept that is used and interpreted in a wide variety of ways depending upon the policy context. Recognizing the absence of a clear, standard definition for CI, CNS devoted part of its initial CI study to help clarify the term's essential meaning. After reviewing all relevant federal policies, reports, and actions that have framed the concept during the last decade, the CNS research team developed the following definition in the context of current discussions relating to terrorism:

> **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 is intended to convey the full scope of the concept as it is currently used by officials at the local, state, and national levels. It reflects three particularly important aspects of critical infrastructure that are significant to current policy discussions:

- *critical infrastructure involves a vast and diverse set of assets that vary from community to community* – these can be difficult to classify into discrete categories because: 1) similar systems can be comprised of many different constituent parts that vary depending on the context in which they are employed; and 2) new categories of CI can emerge, especially as technologies and system relationships change;

- *not all critical infrastructure are similarly "critical"* – CI is, by its nature, related to systems and services that are essential to the functioning of normal life; but what is deemed "essential" will vary according to the community concerned;

- critical infrastructure presents both "physical" (tangible) and "cyber" (data and information related) 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.

This critical chemical infrastructure study again makes use of the same definition of critical infrastructure to provide a clear foundation and starting point for consideration of "chemical" CI.

Critical Infrastructure: The Chemical Industry vs. Chemical Facilities

United States officials considered chemical facilities significant potential terrorist targets well before 9/11.[8] A blue-ribbon panel established to assess the nation's ability to respond to terrorism involving weapons of mass destruction, for example, reported to the President and Congress in 1999 that "a terrorist interested in harming

---

[7] A detailed discussion of the evolution of the term "Critical Infrastructure" may be found in Chapter One (pages 4 to 13) of CNS' "Assessing Terrorist Motivations for Attacking Critical Infrastructure."

[8] See, for example, the Agency for Toxic Substances and Disease Registry's (ATSDR) 1999 report, "Industrial Chemicals and Terrorism: Human Health Threat Analysis, Mitigation and Prevention," <http//www.mapcruzin.com/scruztri/docs/cep1118992.htm>.

large numbers of persons might prefer to attempt to engineer a chemical disaster using conventional means to attack an industrial plant or storage facility, rather than develop and use an actual chemical weapon. In this way, significant technical and resource hurdles could be overcome, as well as reducing the profile of the terrorist organization to potential detection by intelligence or law enforcement agencies."[9] The first formal U.S. policy articulation of chemical infrastructure as part of the nation's "critical infrastructure," however, came only in 2002, when the White House identified the chemical industry in *The National Strategy for Homeland Security* as one of thirteen "critical infrastructure sectors" deserving special protection.[10] Surprisingly, the only rationale clearly articulated in the document for the sector's inclusion as a critical infrastructure was a statement noting that the chemical industry – along with the energy, transportation, banking and finance, and postal and shipping sectors – helps "sustain our economy and touch the lives of Americans every day."[11]

Taken at face value, this brief reference appears to tie the chemical industry's "critical" nature to its unique role in supporting the domestic economy. Yet the Strategy's identification of the Environmental Protection Agency (EPA) as the lead federal agency responsible for coordinating protection of infrastructure relating to the "chemical industry and hazardous materials,"[12] indicates that the federal government was probably equally – if not more immediately – concerned about the toxic nature of the chemicals used in the industry than in the sector's economic significance. Knowing whether to conceive of chemical facilities in an economic context or a safety context is essential for research involving critical chemical infrastructure and terrorism, because the two approaches encompass significantly different potential CI target sets.

If considered strictly in the economic context, the U.S. chemical industry can be characterized as a $454 billion business sector that employs more than one million workers at approximately 13,400 plants and facilities located in all 50 states.[13] Broadly speaking, the chemical industry – as a unique category of business – is involved in the manufacture of organic and inorganic chemicals, the formulation and preparation of chemical-based products (such as pharmaceuticals, paints and explosives), and the use of chemical processes to transform raw materials into intermediate and final products (such as plastics and composite materials). More specifically, the North American Industry Classification System (NAICS) identifies thirty-four specific industry activities that comprise the core of chemical industry business and involve the production of more than 70,000 different products.[14] (Appendix III provides a brief overview of these activities.)

There can be little doubt about the chemical industry's importance to contemporary society. It has been described as "a keystone of the U.S. economy."[15] The thousands of products it provides and multitude of processes it enables are essential inputs to many aspects of today's economy – from agriculture, through fertilizers and pesticides, to the aerospace and defense industries, via coatings and the raw materials needed to build computers. As of 2001, the American chemical industry was the world's largest chemical producer, accounting for more than a quarter of all global chemical production. It accounts for about 2% of the total U.S.

---

[9] Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, "First Annual Report to the President and Congress: Assessing the Threat," December 15, 1999, <http:///www.rand.org/nsrd/terrpanel/terror.pdf>.
[10] As noted by the Congressional Research Service, a public White House document outlining the Bush Administration's position on the 2001 USA PATRIOT Act included the chemical industry as an example of a critical infrastructure as early as October 2001. The document, however, was not a formal articulation of policy regarding critical infrastructure. See John Motef et al., "Critical Infrastructures: What Makes an Infrastructure Critical?" Congressional Research Service, January 29, 2003, p. 14.
[11] White House, National Strategy for the Physical Protection of Critical Infrastructures and Key Assets," February 2003, p. 30.
[12] *Ibid,* p. 32.
[13] According to the U.S. Department of Energy, "most of the basic chemicals production [in the U.S.] is concentrated along the Gulf Coast, where petroleum and natural gas feedstocks are available in refineries. Production of other products such as plastics, pharmaceuticals, and fertilizers is more widely dispersed among the states." 1998 Chemical Manufacturers Association figures further indicate that ten states – California, Illinois, Louisiana, New Jersey, New York, North Carolina, Ohio, Pennsylvania, South Carolina, and Texas – account for 62% of chemicals production and 60% of chemical industry employment in the nation. See <http//www.oit.doe.gov/chemicals/profile.shtml>.
[14] U.S. Census Bureau, "2002 NAICS Codes and Titles," <http://www.census.gov/epcd/naics02/def/NDEF325.HTM#N325>.
[15] Department of Energy, "Industry Profile," < http://www.oit.doe.gov/chemicals/profile.shtml.>

GDP and nearly 12% of the manufacturing GDP. Understood in this context, any physical aspects of the chemical industry that could be damaged in a way that would impede the industry from continuing its support of the economy might be considered critical infrastructure. Facilities within the chemical industry that are captured by such a definition of "chemical critical infrastructure" would include but not be limited to: corporate headquarters, production plants, specialized transportation facilities and vehicles, and storage facilities.

It is important to note, however, that if critical chemical infrastructure is understood in such an economic context some facilities considered "critical" might have no direct relation to large quantities of toxic industrial chemicals at all. For example, a corporate headquarters that plays an essential logistics role in running day-to-day operations of chemical plants in other locations might be considered critical infrastructure, even though the facility itself might consist of little more than an office building. At the same time, a facility containing massive quantities of TICs – such as a chemical wholesaler distribution center – would not be considered critical chemical infrastructure, because wholesale activities are considered business activities outside the scope of formally defined chemical manufacturing.

If, on the other hand, chemical critical infrastructure is to be deemed "critical" because of safety concerns related to the presence of high concentrations of hazardous or volatile chemicals at specific facilities, a different set of chemical CI targets emerge. Although no definitive open source study has been completed that identifies the exact number of such facilities in the nation, the EPA estimated in the mid-1990s that some 66,000 facilities throughout the United States use or store significant quantities of one or more toxic or flammable substances that have been identified by the EPA and Congress as posing the "greatest risk of causing death, injury, or serious adverse effects to human health or the environment" if accidentally released.[16] (See Box 1.1) When flammable fuels are removed from this figure, roughly 33,000 facilities were still estimated to have significant quantities of toxic chemicals on site. Notably, many of these facilities fall outside the scope of what is recognized – in terms of business activities – as the chemical industry.

A 2000 study of data from more than 15,000 facilities that submitted chemical accident prevention and preparedness plans as part of the federal government's Risk Management Program (RMP), for example, indicates that 13 of the 20 most frequently occurring chemical processes involving significant quantities of extremely hazardous substances took place in industries <u>other than</u> the NAICS-defined chemical industry. (See Appendix IV for a list and brief explanation of these processes by business industry.) This suggests that if chemical critical infrastructure is to be understood in the context of safety as related to TICs, chemical CI facilities will be found both in and outside what has traditionally been recognized as the chemical industry. At the same time, such an understanding would mean that some facilities within the chemical industry – specifically those that don't involve the immediate presence of high quantities of toxic industrial chemicals (a corporate headquarters, again, serves as a good example) – might <u>not</u> be considered critical infrastructure.

To date, the U.S. government has been less than clear regarding how it defines critical chemical infrastructure. As mentioned previously, the 2002 *National Strategy for Homeland Security* discusses "chemical industry" critical infrastructure in decidedly economic terms, although it also links the chemical industry with hazardous materials for purposes of bureaucratic responsibility. The 2003 *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets* introduces its discussion of "chemical industry and hazardous material" critical infrastructure by again emphasizing the economic importance of the chemical industry sector,[17] but it later notes that,

---

[16] See James C. Belke, "Chemical accident risks in U.S. industry – A preliminary analysis of the accident risk data from U.S. hazardous chemical facilities," U.S. EPA, September <http://www.epa.gov/ceppo/pubs/stockholmpaper.pdf>.

[17] "Energy, transportation, banking and financial services, *chemical manufacturing,* postal services, and shipping sustain the Nation's economy and make possible and available a continuous array of goods and services." (Emphasis added.) See White House, "The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets," February, 2003, p. 6.

Box 1.1**

HOW MANY CHEMICAL FACILITIES DO WE HAVE?

How many chemical facilities are located in the United States? A short, reliable answer to this question is: "Thousands." A more precise answer, however, is: "The exact number is publicly unknown." In discussions concerning terrorism and critical chemical infrastructure, three figures are most frequently referenced – often inaccurately – to describe the size of such infrastructure in the U.S.: 66,000 facilities; 33,000 facilities; and 15,000 facilities. Where do these numbers come from and which is the most accurate? It depends on what is being discussed:

66,000 Facilities. In the aftermath of the tragic chemical accident in Bhopal, India that killed thousands and injured even more (see Section 3 for a detailed discussion of this incident), Congress passed a series of laws designed to minimize the consequences of unintentional TIC releases in the United States. In one of these – the 1990 Clean Air Act (CAA) – Section 112(r) established a risk management program, which requires facilities dealing with certain quantities of hazardous substances to prepare and submit Risk Management Plans (RMPs) to the EPA. The RMPs must "summarize the potential threat of sudden, large releases of certain chemicals, including the results of off-site consequence analysis (OCA) for a worst-case chemical accident."[18] EPA initially identified "77 acutely toxic substances, 63 flammable gases and volatile flammable liquids, and 'highly explosive substances'"[19] that – if produced, used or stored at a site in quantities above certain threshold amounts – would require an RMP. *According to internal analysis, the EPA estimated that about 66,000 facilities would be subject to the risk management program given these specific criteria.*[20]

33,000 Facilities. After intensive lobbying by the propane industry, in March 2000 "Congress prohibited the EPA from regulating under the [CAA mandated] risk management program any listed flammable substance when used as fuel or held for sale as fuel at a retail facility."[21] Since roughly half of the 66,000 facilities the EPA originally estimated to require RMPs possessed only "listed flammable fuels" on site, EPA revised the number of facilities it expected to be regulated by Section 112(r) to 33,000.

15,000 Facilities. In 2000 James Belke, an official in EPA's Chemical Emergency Preparedness and Prevention Office, prepared a paper summarizing initial risk management program data from "approximately 15,000" facilities that had submitted reports by September of that year. A footnote in the document notes that the discrepancy between the 33,000 facility estimate and the 15,000 facilities that had submitted RMPs was likely due to three factors. "First, significant anecdotal information suggests that a large number of facilities took actions to avoid being regulated under the program. Such actions include reducing chemical inventory below the regulatory threshold, replacing a regulated substance with a non-listed substitute, or eliminating the covered process altogether. Second, EPA may have overestimated the number of facilities subject to regulation. Third, some facilities may have not yet complied with regulation."[22]

As these explanations make clear, the exact number of facilities possessing TICs remains uncertain. Policymakers concerned with safety issues relating to TICs might be predisposed to follow the Precautionary Principle and use the larger 66,000 facility figure. Indeed, this is the number of chemical facilities identified in the *2003 National Strategy for the Physical Protection of Critical Infrastructure and Key Assets*. It is notable, however, that this figure is only an EPA estimate and one that is now almost ten years old. The 15,000 facility figure is the one most commonly used in discussions relating to terrorism, because it is often referenced in the context of worse-case chemical accident scenario statistics taken from Belke's report. (This figure is also closest in size to the 13,400 facilities claimed by the Chemical Manufacturers Association in 1997.) Use of this smaller figure, however, probably significantly understates the number of TIC facilities located across the country that pose safety risks if attacked by terrorists.

CNS researchers are inclined to believe that critical chemical infrastructure should be thought of in the context of the largest figure, for the simple reason that terrorists are more likely to think broadly and creatively about targets, rather than within the context of bureaucratically defined categories. That said this is a matter that is clearly worth additional research and quantitative analysis.

[18] Schierow, *Chemical Plant Security*, p. 15.
[19] *Ibid.*
[20] Belke, "Chemical Accident Risks in U.S. industry – A preliminary analysis of accident risk data from U.S. hazardous chemical facilities," pp. 6-7.
[21] *Ibid*, p. 7.
[22] *Ibid*, p. 7.

> "In addition to the economic consequences of a successful attack on this sector, there is also the potential of a threat to public health and safety. Therefore the need to reduce the sector's vulnerability to acts of terrorism is important to safeguard our economy and protect our citizens and the environment."[23]

A footnote in the report further clarifies that certain chemical and hazardous material facilities may be considered "key assets" – "targets whose destruction would cause large-scale injury, death, or destruction of property, and or profoundly damage our national prestige and confidence"[24] – and that "their specific protection issues relate to the entire [chemical] sector."[25] Such language suggests strongly that chemical facilities in and outside the traditional chemical industry – for both economic and safety reasons – can be considered critical infrastructure.[26]

Finally, it is worth noting that while other parts of the federal government have also remained unclear about the exact definition of chemical industry critical infrastructure, in matters concerning possible terrorist attacks they have tended to emphasize safety rather than economic issues relating to chemical facilities. In early 2004, for example, both the General Accounting Office and Congressional Research Service addressed terrorism vulnerability issues associated with chemical facilities writ large – not just within the chemical industry – and primarily in the context of unintentional releases of toxic industrial chemicals, not in terms of how such attacks might undermine the economy.[27] Even more noticeably, draft Senate legislation known as the "Chemical Security Act" acknowledges the unique role of the chemical industry as part of critical infrastructure, but focuses nearly all of its attention on regulating the security of "chemical sources" to prevent unintentional release of "hazardous substances."[28] It does so almost entirely without regard to whether the chemical sources are owned or operated within the chemical industry sector or other sectors. (See Box 1.2.)

Given the current lack of a clear, standard definition for what is meant by critical infrastructure relating to the chemical industry in contemporary policy discussions, CNS crafted the following one to guide its research:

> **Critical chemical infrastructure consists of those physical facilities that either: 1) the chemical industry – as defined by the NAICS – depends on to provide minimum essential levels of services and products; or 2) contain chemicals in sufficient quantities that if successfully attacked could significantly jeopardize public health and safety in surrounding communities.**

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 "chemical" critical infrastructure that have been raised in the context of policy discussions relating to terrorism to date; namely:

---

[23] *Ibid*, p. 65.
[24] *Ibid*, p. 7.
[25] *Ibid*, p.66.
[26] It is worth observing that the 2003 critical infrastructure strategy contains a box that highlights the extent of the nation's critical infrastructure "Protection Challenges" for different sectors. (*Ibid*, p. 9.) This box notes that 66,000 chemical plants require protection. Although not sourced, it is likely that this figure is the same EPA estimate discussed previously, which approximates the number of facilities in all sectors that used or stored significant quantities of highly toxic or flammable substances in the mid-1990s. This would suggest that the government may also be considering facilities that store large quantities of fuels, such as propane, in its consideration of chemical industry and hazardous materials critical infrastructure. (Nuclear power plants are clearly treated as a separate category in the report and are not included under the rubric of hazardous materials.)
[27] See Congressional Research Service report, " Chemical Plant Security," January 20, 2004 and statement by John Stephenson, "Federal Action Needed to Address Security Challenges at Chemical Facilities," General Accounting Office, February 23, 2004.
[28] See S.157 "The Chemical Security Act of 2003," <http://www.theorator.com/bills108/s157.html>.

- *"chemical" critical infrastructure involves assets that may be found both within and outside the traditionally defined chemical industry* – to minimize the semantic confusion and ambiguity that, as discussed earlier, can be associated with the terms "chemical industry critical infrastructure" and "chemical industry and hazardous materials critical infrastructure," CNS deliberately refers to critical infrastructure related to the chemical industry and large quantities of toxic industrial chemicals as "critical chemical infrastructure";

- *critical chemical infrastructure is significant for economic and safety reasons* – we depend on critical chemical infrastructure to maintain our economy and way of life; we also depend on such infrastructure for the safe management and appropriate use of chemicals that are often extremely toxic and/or volatile;

- *critical chemical infrastructure involves more than chemical manufacturing plants* – critical chemical infrastructure involves numerous types of assets, including but not limited to: corporate headquarters, manufacturing and processing plants, specialized transportation vehicles (such as rail tank cars, tank trucks, pipelines, and barges and ships), and storage facilities.

Box 1.2*

"FINDINGS" FROM DRAFT SENATE LEGISLATION
S. 157 – THE CHEMICAL SECURITY ACT

Sec.2. Findings.

Congress finds that –

(1) the chemical industry is a crucial part of the critical infrastructure of the United States --

(A) in its own right; and

(B) because that industry supplies resources essential to the functioning of other critical infrastructures;

(2) the possibility of terrorist and criminal attacks on chemical sources (such as industrial facilities) poses a serious threat to public health, safety, and welfare, critical infrastructure, national security, and the environment; and

(3) the possibility of theft of dangerous chemicals from chemical sources for use in terrorist attacks poses a further threat to public health, safety, and welfare, critical infrastructure, national security, and the environment…

(4) there are significant opportunities to prevent theft from, and criminal attack on, chemical sources and reduce the harm of such acts…

*S.157 – Establishing The Chemical Security Act of 2003, January 14, 2003, <http://www.theorator.com/bills108/s157.html>.

D. Structure of Report

The remainder of this report is divided into four additional sections. The next section, Section 2, reviews the findings of a literature assessment to examine how issues relating to chemical CI have been framed since 9/11 and in the context of the current "War on Terrorism." In particular, it provides an overview of a number of recent incidents that demonstrate the reality of terrorist interest targeting chemical critical infrastructure. (These incidents, for methodological reasons, are not captured in the Critical Infrastructure Terrorism Incident Catalog – CrITIC – which is discussed later in the report.) Section 2 also identifies a range of qualities and aspects of chemical CI, which are referenced in recent literature as factors that likely shape terrorist motivations for attacking such targets. Section 3 reviews the purpose and methodology of CrITIC and presents a summary of the limited number of chemical CI cases it has captured. In Section 4, the findings of Sections 2 and 3 are synthesized to refine the DECIDe (Determinants Effecting Critical Infrastructure Decisions) Framework for specific terrorist group assessments relating to critical chemical infrastructure issues. Section 5 summarizes the study's key findings and suggests avenues for further research.

Section 2

CRITICAL CHEMICAL INFRASTRUCTURE IN THE CONTEXT OF CONTEMPORARY TERRORISM

A. Literature Assessment Overview

To establish a theoretical foundation for studying terrorist motivations for attacking critical chemical infrastructure, CNS reviewed a wide body of terrorism-related, threat assessment-focused, and industry-specific literature. The assessment sought to: 1) glean expert consensus regarding terrorist target selection; 2) identify analytical approaches that might be valuable to those seeking to understand such terrorist group decision making processes; and 3) understand unique aspects of critical chemical infrastructure that might markedly influence terrorist targeting of chemical facilities.

Most of the materials considered in this process were initially evaluated as part of the research done for CNS' first study concerning terrorist motivations for attacking CI. These included 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. The assessment (which is discussed in detail in Chapter 2 of the first report and summarized in the "Literature Assessment" section of Appendix II at the end of this report) confirmed that little existing work focuses specifically on the reasons why terrorists choose to attack critical infrastructure targets. 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.

The literature, however, was essential in helping 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).

Appendix I of this report clarifies the meanings of these factors by presenting the terminological definitions from the first study.

A very small amount of literature – primarily consisting of government reports, chemical industry analyses, studies by environmental organizations, and news exposés – specifically addresses the threat of terrorist attacks on chemical facilities. Most of these materials were produced after 9/11 and focus on either the possible effects of a successful terrorist attack against a chemical facility or the existing security vulnerabilities of chemical facilities. Besides highlighting the potentially massive destructive potential of such attacks, virtually none of this literature examines terrorist motivations for attacking chemical facilities in any depth.[29] The discussions found in these documents, however, provide important insight into how the issue of critical chemical infrastructure might best be understood in the context of contemporary terrorism. In particular, the literature indicates: 1) the reality of terrorist interest in attacking chemical facilities; and 2) the wide range of objectives terrorists might have for attacking critical chemical infrastructure. The following portions of this section present the major findings CNS researchers identified relating to these issues.

B. Terrorist Interest in Critical Chemical Infrastructure Targets

In June 2004, the National Commission on Terrorist Attacks Upon the United States issued a staff statement that included among its key conclusions the finding that "al Qaeda [*sic*] may seek to conduct a chemical attack by using widely-available industrial chemicals, or by attacking a chemical plant or a shipment of hazardous materials."[30] Although treated at the time as breaking news by numerous media outlets, this same observation was made publicly more than two years earlier by former Director of Central Intelligence George Tenet when he testified before the Senate Armed Services Committee that "al Qa`ida or other terrorist groups might try to launch conventional attacks against the chemical or nuclear industrial infrastructure of the United States to cause widespread toxic or radiological damage."[31]

The use of "may" and "might" in the two statements suggests that both conclusions are speculative. Oblique references from other security officials, however, indicate that the United States and other governments might be more concretely aware of terrorist interest in attacking critical chemical infrastructure than they are acknowledging. In February 2003, for example, the U.S. Department of Homeland Security's National Infrastructure Protection Center issued a Homeland Security Information Update that warned, "Al Qa`ida operatives… may attempt to launch conventional attacks against the U.S. nuclear / chemical-industrial infrastructure to cause contamination, disruption, and terror. *Based on information*, nuclear power plants and industrial chemical plants remain viable targets."[32] (Emphasis added.) More recently, in February 2004 Rudolf Adam, the deputy director of Germany's Federal Intelligence Service commented that his organization had "unspecified hints that plans have been made [by al Qa`ida] or are still under way to target the chemical industry and chemical infrastructure."[33]

---

[29] Some terrorism literature, such as Jonathan Tucker's *Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons* and Richard Falkenrath et al.'s *America's Archilles' Heel: Nuclear, Biological and Chemical Terrorism and Covert Attack*, deals with terrorist motivations for using chemical weapons. While providing some important background information, these materials do not consider terrorist motivations for attacking critical infrastructure or chemical facilities directly.

[30] National Commission on Terrorist Attacks Upon the United States, "Overview of the Enemy," Staff Statement No. 15, June 16, 2004, p. 12, <http://www.9-11commission.gov/staff_statements/staff_statement_15.pdf>.

[31] George J. Tenet, "Worldwide Threat – Converging Dangers in a Post 9/11 World," Testimony before the Senate Armed Services Committee, March 19, 2002, <http://www.cia.gov/cia/public_affairs/speeches/2002/senate_select_hearing_03192002.html>.

[32] National Infrastructure Protection Center, "Al Qa`ida Chemical, Biological, Radiological, and Nuclear Threat and Basic Countermeasures," Homeland Security Information Update, February 12, 2003, <http://www.esisac.com/publicdocs/DHS/NIPC%20Bulletin%2003-003%20Final.pdf>.

[33] Reuters, "Al Qaeda under pressure for new strike – spy chief," February 11, 2004, <http://au.news.yahoo.com/040210/15/nnqa.html>.

While open source information has not yet definitively identified the full scope of current terrorist interest in targeting critical chemical infrastructure, a careful review of literature from the last five years yields clues that indicate that at least some terrorist groups are actively looking into such attack options. The following five incidents (listed in reverse chronological order) serve as important recent examples of the types of evidence that suggest that an ideologically broad range of domestic and foreign terrorist organizations are considering chemical facilities as potential targets.

- *Al Qa`ida Chemical Industry Literature.* An often cited, potentially vivid demonstration of al Qa`ida's interest in the American chemical industry was the December 2001 discovery of U.S. chemical trade publications in "an Osama bin Laden hideout" in Afghanistan.[34] Senator Christopher Bond cited this fact as "chilling confirmation" of the terrorist group's interest in attacking chemical facilities to cause "mass casualties" and "widespread destruction" when he advocated an amendment to the Clean Air Act that would limit public access to sensitive chemical plant consequence management information.[35]

- *Alleged Tennessee Chemical Plant Fly-Over.* In early 2001, Muhammad Atta – the al Qa`ida ringleader of the September 11, 2001 attacks – may have conducted a reconnaissance flyby over a specialty chemical plant in Copperhill, Tennessee. After 9/11, a local resident reported to federal law enforcement authorities that he recognized Atta as an out-of-town pilot who had landed in Copperhill in March. The pilot, who called himself "Mo," had spoken to the resident and expressed persistent interest in the nearby Intertrade Holdings chemical facility that he had seen from air. Specifically, the pilot asked the resident repeatedly about the chemicals stored in the massive storage tanks on the plant site. The resident incorrectly told the pilot that the tanks were empty. In fact, as much as 250 tons of sulfur dioxide were likely in the tanks at the time, which if released could have endangered 60,000 people living in the surrounding area with death or serious injury. In October 2001 the FBI publicly acknowledged that it received two reports of Atta being in the area, but the Bureau declined to confirm his presence there.[36]

- *Twin Sisters Plot.* Two men associated with right-wing groups such as the Montana Freemen, Nevada Freedom Coalition, and Texas Constitutional Militia were arrested in December 1999 for plotting to blow up a massive propane storage facility near Sacramento, California. The Elk Grove facility, which is owned by Suburban Propane, holds 24 million gallons of propane and handles nearly 15% of all propane sold in California.[37] Much of the propane at the site is stored in two 122-foot-tall tanks, which one of the conspirators referred to as the "twin sisters." A threat assessment of the facility prepared for the FBI by Lawrence Livermore National Laboratory concluded that a successful attack on either tank "would likely result in a firestorm that could reach as far out as 14 kilometers from the site and could cause a fatality rate as high as fifty percent up to five miles away."[38] An informant told authorities that the conspirators wanted to conduct this and other attacks near the end of the millennium to "force authorities to declare martial law, potentially whipping up public unrest and helping the militia overthrow the U.S. government."[39] The conspirators were arrested before the attack could be carried out.

---

[34] James V. Grimaldi and Guy Gugliotta, "Chemical plants are feared as targets: concerns grow that terrorists might hit toxic inventories," Washington Post, December 16, 2001, <http://www.mapcruzin.com/news/rtk121501a.htm>; Kathleen McFall, "Nationwide Chemical Sites Are Targets of Opportunity," December 1, 2003, <http://www.construction.com/NewsCenter/Headlines/ENR/20031201a.asp>.
[35] Christopher Bond, "Statement on S.2579," Congressional Record, June 5, 2002, <http://www.fas.org/sgp/congress/2002/s060502.html>.
[36] See: Grimaldi et al., 2001; John Fialka, Tom Hamburger and Gary Fields, "Hijackers interest in crop dusters still puzzles terrorism investigators," Wall Street Journal, November 11, 2001, <http://www.freerepublic.com/focus/f-news/574221/posts> ; Joel Engelhart, "From terrorist to spy, Atta's mission was extensive," The Palm Beach Post, October 29, 2001, <http://www.ctcintl.com/10292001.shtml>; and Associated Press, "Hijacker may have scouted Tenn. chemical plant," St. Petersburg Times, October 19, 2001, <http://www.sptimes.com/News/101901/Worldandnation/Hijacker_may_have_sco.shtml>.
[37] Doug Willis, "FBI arrests suspects in alleged bomb plot," AP, December 4, 1999.
[38] As quoted by Jennifer Kerr, "Alleged propane plot tied to plan to overthrow U.S. government," The Sacramento Bee, December 7, 1999, <http://www.freerepublic.com/forum/a384cc4765cac.htm>.
[39] *Ibid.*

- *Operation SOURGAS.* In 1997 the FBI infiltrated a four-member Ku Klux Klan group planning to blow up a hydrogen sulfide tank at a refinery near Dallas, Texas. The members planned to use an improvised explosive device at a Mitchell Energy Corp. plant to release a lethal cloud of "sour gas." Although the ultimate objective of the group was to use the explosion to divert law enforcement so that KKK members could commit a crime on the other side of town, the group estimated that 2,000 people – close to half the local community's population – would be affected[40] and that hundreds of area residents, including children, might die. The conspirators were arrested before the attack could be carried out.[41] (See Box 2.1.)

- *Chechen Polymer Materials Works Attack.* In 2000, the U.S. Department of Justice referenced 1995 press accounts of Chechen terrorists threatening to blow up a polymer plant in Budennovsk, Russia as an example of international terrorists seeking to release toxic industrial chemicals.[42] On the first day of the bloody Budennovsk hostage crisis in June of that year, ITAR-TASS did, indeed, report that "the terrorists, who are clearly linked to illegal Chechen armed formations, planned to blow up a polymer materials works in Budennovsk and trigger an ecological disaster in the region. TASS learned this from well-informed sources."[43] Although, the BBC repeated the identical story two days later on its World Broadcasts program, the actual hostage crisis played out publicly in a Budennovsk hospital complex and not in a chemical plant. Without additional information it is impossible to determine if the terrorists actually sought to attack – or use the threat of such an attack – to leverage their negotiating position with the Russian government during the [two-week] crisis.

Because these five cases did not result in actual attacks against chemical facilities, they – for methodological reasons – were not included in the Critical Infrastructure Terrorist Incident Catalog (discussed in Section III) which CNS developed to track CI terror attacks. That they are discussed in the context of this literature assessment rather than in the case studies presented later in the report, however, does not diminish their significance as warnings and indicators that a variety of terrorist groups – both at home and abroad – likely consider chemical CI a high-value target for a broad range of reasons.

[Chapter text continues after box on pages 15-16.]

[40] Russell Chisholm, "Weapons of Mass Destruction: Threat Overview," FBI presentation, <http://www.dartmouth.edu/~engs05/readings/md/wmd/WMDHTML/sld011.htm>.
[41] Robert Burnham, "Statement for the Record," U.S. Senate Subcommittee on Clean Air, Wetlands, Private Property and Nuclear Safety, March 16, 1999, <http://www.fas.org/irp/congress/1999_hr/990316-senlast.htm>.
[42] Department of Justice, 2000, p. 24.
[43] "Hostages, Facilities Seized in Budennovsk; Buddennovsk attackers "planned to blow up polymer works," ITAR-TASS, June 14, 1995.

Box 2.1

OPERATION SOURGAS

In April 1997, the FBI arrested four individuals for plotting to destroy a gas well in an effort to release a large, lethal quantity of hydrogen sulfide (also known as "sour gas") into inhabited sections of Wise County, Texas.[44] The case has drawn the attention of policymakers and law enforcement officials not only because three of the four perpetrators were members of the Ku Klux Klan (KKK), but also because the four expected to use toxic chemicals associated with the plant to kill an estimated 2,000 people.[45] The following description provides a summary of the episode and a brief discussion of the perpetrators' motives.

After the 1995 Alfred P. Murrah Federal Building bombing, the FBI established a North Texas Joint Terrorism Task Force that investigated possible domestic terrorists in an area that included Wise County.[46] In March 1997, the task force learned from an informant that members of a branch of the KKK – The Invisible Empire, True Knights of the Ku Klux Klan – were planning "something big… that would involve a lot of dead people." [47] Following an investigative operation codenamed "SOURGAS," the task force concluded that four individuals were planning to attack the Mitchell Energy Plant located in Wise County in order to create a diversion that would allow them to rob an armored car in nearby Chico, Texas.[48] On April 22, 1997, the FBI arrested four suspects – Carl Waskom, Jr., Edward Taylor, Jr., and Shawn and Catherine Adams – charging them with conspiracy to commit armed robbery and possession of illegal weapons.[49] Two years later, all four were convicted of the charges and sentenced to prison.[50]

The conspirators' plot was simple in design. It called for fastening three explosives to three separate gas tanks at the Mitchell facility.[51] One of the devices was to have been placed in an obvious location that would be easy for police to spot. The other two explosives were to be hidden from view. The group also planned on hiding several smaller bombs in trees near the plant. The group hoped to lure law enforcement officials to the plant by calling in a bomb threat. Once there, the conspirators hoped the police would focus on the one "visible" bomb and would fall to the other two hidden bombs when detonated.

The group erroneously expected that the Mitchell facility contained hydrogen sulfide and that the explosions would generate a toxic cloud of 'sour gas.' Simultaneous to the planned detonation of the gas tanks, the group planned on discharging the explosives hidden in the surrounding tree, "in order to set the surrounding forest afire."[52] FBI Special Agent Robert Garrity reported that, "if their plan was successful, they anticipated they might wipe out half of Wise County."[53] Significantly, even if the bombs had been detonated the resulting explosion would have been entirely conventional as the plant, according to Mitchell Energy and Development Corp. Director of Public Affairs, Brian Engel, stored no hydrogen sulfide.[54]

The conspirators' motivations for the attack were both tactical and strategic. In the short-term the group intended to use the attack as a diversion while it robbed an armored truck of a putative $2 million. In the long-term the perpetrators planned on using the money to finance a "race-war."[55] Tape recordings obtained by an FBI mole revealed that the group viewed themselves as, "the last line of defense against gangs and drug dealers in a world where the police have been emasculated by minority rights.[56] Such beliefs conform to elements of the KKK's general ideology.

---

[44] Jim Schutze, "Four Accused of Plot to Blow Up Gas Plant; Armored Car Robbery Part of Plan," *Houston Chronicle*. 24 April 24, 1997, p. A1.
[45] Chisholm, "Weapons of Mass Destruction: Threat Overview."
[46] Christine Biederman "Ku Klux Klowns," *Texas Monthly*, January 1998, p.58.
[47] Biederman, "Ku Klux Klowns," p. 59. Justin Bachman and Laura Vozzella "FBI Says Bomb Plot Thwarted; Gas Blast Could Have Wiped Out 'Half of Wise County'," *Fort Worth Star-Telegram*, April 24, 1997, p.A1.
[48] *Ibid.*
[49] Biederman, "Ku Klux Klowns."
[50] Taylor was sentence to 22 years in federal prison, while Shawn Adams received 14 years, his wife, Catherine received 15 years, and Waskom received nine. Laura Vozzella "Sentences For Four Would-Be Bombers Too Tough Court Says," *Fort Worth Star-Telegram*, June 24 1999, Metro, p. 4
[51] The group had tested two bombs at a local nature preserve. Apparently one of the devices worked as intended while the other one was a "dud." Schutze, "Four Accused of Plot to Blow up Gas Plant."
[52] *Ibid.*
[53] *Ibid.*
[54] Justin Bachman and Laura Vozzella "FBI Says Bomb Plot Thwarted; Gas Blast Could Have Wiped Out 'Half of Wise County'," *Fort Worth Star-Telegram*, April 24, 1997, p. 1
[55] Biederman, "Ku Klux Klowns."
[56] *Ibid.*

Box 2.1

OPERATION SOURGAS (Continued)

Under the previously mentioned moniker of "The Invisible Empire, True Knights of the Ku Klux Klan" three of the four suspects held official KKK roles. Taylor was an Imperial Wizard, Adams an Imperial Night Hawk (security guard), and his wife, Catherine, head of the ladies auxiliary. Waskom, the fourth perpetrator, was not formally affiliated with the KKK.[57]

Had law-enforcement not intervened it is doubtful that the assault would have succeeded in any of its goals. Subsequent raids on the perpetrators mobile homes netted no explosives and eight dummy hand grenades.[58] Financially the four would have needed some external source of funds to finance the operation as between the four of them, their cash assets, at the time of their arrests, totaled $51.34.[59] Court proceedings revealed that the four had planned on robbing two local drug-dealers and using that money to finance the attack on the Mitchell Plant and assault on the armored car.[60]

In sum, the Wise County KKK case illustrates the role that both ideology and practical considerations can play in the formulation of a chemical facility attack plan. While the putative gas release would have served an initial tactical need (distracting law enforcement), it would have also helped enable the perpetrators, had they been successful, to pursue a "race war" with considerable financial resources.

Another set of incidents that was revealed in the literature assessment process, but not CrITIC – again for methodological reasons – were attacks on chemical facilities that took place in the context of armed conflicts. Although not undertaken by terrorists per se, a variety of such attacks against chemical CI were conducted by warring parties during the recent Balkan war. These incidents provide a unique and concrete insight into the motivations actors have had in the past for targeting critical chemical infrastructure. A brief overview of attacks carried out by Serbian forces against Croatia's Petrokemija plant between 1993 and 1995 is presented here as a representative example of what lessons analysts might glean from actual assaults carried out on chemical facilities in a military context that they might miss from cases that were simply planned or later thwarted.[61]

- *Serb Attacks on Petrokemija.* Petrokemija is located in the town of Kutina, in central Croatia. Although best known as one of Europe's largest producers of fertilizers, the plant also produces light fraction petroleum products and carbon black. On a regular basis, Petrokemija produces and stores such hazardous substances as formaldehyde, heavy oils, sulfur, and nitric, sulfuric and phosphoric acids.

  Serbian forces attacked Petrokemija on six separate occasions between 1993 and 1995.[62] The attacks gradually increased in intensity – first machine guns, then multiple rocket launching systems, then artillery, and finally warplanes armed with bombs were used to attack the site.

---

[57] Jim Schutze and Richard Stewart, "Texas Bomb Plot Suspects Klan Officers, Group Says," April 25, 1997, *Houston Chronicle*, p. A1. See also, "Calendar of Conspiracy, Volume 1, Number 4: A Chronology of Anti-Government Extremist Criminal Activity, October to December 1997," Anti-Defamation League, February 18, 1998.

[58] While under surveillance the four "puffed outrageously" about their supply of C-4 plastic explosives, Chinese-made assault rifles and two 55 gallon drums filled with "superdupper explosives" from Chicago. None of these items were ever found although authorities believed that the group was actively seeking them... Biederman, "Ku Klux Klowns."

[59] *Ibid.*

[60] *Ibid.*

[61] Several other noteworthy Balkan cases exist. The Pliva Pharmaceutical Factory in the Croatian capital of Zagreb was putatively targeted by Serbian war-planes. Replete with ammonia and chlorine – irritants and choking agents respectively – Croatian authorities concluded that a successful attack on the plant would have unleashed a "toxic cloud with a 50 percent lethality" extending more than 3 km from the plant. Also noteworthy is that Serbian forces did strike a major Croatian chemical facility near the town of Jovan. The attack resulted in the release of 72 tons of anhydrous ammonia, leading to the evacuation of over 30,000 civilians. See "Weapons of Mass Destruction, Toxic Industrial Materials, and the Use of Obscuration," in, *Combined Arms Operations in Urban Terrain*, Department of the Army Field Manual, No. 3-06.11. Appendix F, February 28, 2002; and Theodore Karasik, *Toxic Warfare*, RAND 2002, pp. 21-22.

[62] U.S. 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, p. 24.

The Serbs were so determined to destroy the facility that in 1995 they began efforts to modify an extremely powerful naval missile system for a terrestrial attack mission against the plant.[63]

Despite a pre-war federal system that recognized three "nations" within the confines of Yugoslavia – Serbs, Croats, and Muslims – the Balkan conflict of the 1990s was in many ways a civil war. As such, Serbian military officials had access to detailed descriptions of Petrokemija and its surrounding environs.[64] Moreover, given the nature of civil conflict, it can be assumed that some Serbian military forces had first-hand knowledge of the target environment. Given this situation, it is notable that the Serbs were ultimately not successful in their attempts to destroy Petrokemija.

Croatian officials were quick to recognize the plant's vulnerability after the initial Serbian attack. By late 1993, the Ministry of Defense had "organized special fire brigades and hazardous materials response units; conducted mass casualty training exercises; stationed a Croatian army field decontamination unit near the plant; created special helicopter fire suppression and casualty evacuation units; and prepared local emergency rooms to treat contaminated patients."[65] *C*oupled with "well-organized antiaircraft defenses," these measures (i.e. special fire suppression units and training) prevented Serbian military forces from succeeding in their efforts to destroy the plant.[66]

Subsequent studies by the Croatian government have concluded that had Serbian forces been successful in creating a massive fire at the plant, anyone living within a 100 kilometer radius of Kutina would have been endangered.[67] Echoing these conclusions, Petrokemija's Chairman of the Board, Boris Mesaric, revealed in 1998 that if the plant's main storage tank – which contained 10,000 tons of liquid ammonia – had been compromised, "a great ecological disaster" would have ensued and "surely nobody in Kutina, and the surrounding area, would have survived." [68]

It should be noted, however, that no formal studies of the Petrokemija attacks have been conducted by non-Croatian entities. Consequently, it is quite possible – especially in the emotionally charged context of the analysis – that these casualty estimations are too high. Indeed, given the nature of the chemicals present and the manner in which they would have been dispersed, these casualty and contamination estimates could only have been approximated if several precise environmental factors had been considered (most importantly, weather conditions). Still, based on the quantity of TICs present, and the firepower and logistics available to the attacking Serbs, an immense fire at Petrokemija would certainly have had severe consequences for the immediate Kutina region.

Serb motivations for the attacks are widely attributed to their "ethnic cleansing efforts."[69] Indeed, Petrokemija's wartime director is explicit in stating that Serbia undertook attacks against the facility with the goal of "killing civilian non-Serbs living in the area."[70] Throughout the Balkan conflict, Serbian leaders were publicly open about their "responsibility to cleanse the greater Serbia."[71]

---

[63] Department of Justice, 2000. This assault, however, never took place. NATO planes destroyed the system as it underwent modifications in Serbian held Bosnia. Ricardo Cappelli and Nicola Labanca, "Proliferation and Disarmament of Chemical Weapons in the NATO Framework: Lessons from History." University of Sienna, 2000.

[64] Aileen McCabe, "Balkans: Bombs Rain as Leaders Meet to Discuss Peace," *Ottowa Citizen*, September 8, 1995, p. A6.

[65] Department of the Army, "Weapons of Mass Destruction, 2002.

[66] Boris Mesaric, 19, October 2004. Personal email.

[67] Such a radius of contamination, Croatian officials claimed, would have extended into Italy and Hungary.

[68] "Chemical Warfare Conventions Changed Over Fertilizer Plant Attacks," *Washington Times International Reports.net*, December 1998. <http://www.internationalspecialreports.com/europe/01/croatia/chemicalwarfare.html>.

[69] "These facilities were in close proximity to population centers and appeared to have been chosen for that reason." Department of Justice, 2000, p. 24.

[70] Boris Mesaric, Chairman of the Board, Petrokemija, telephone interview, September 13, 2004.

[71] See, V.P. Gagnon Jr., *The Myth of Ethnic War: Serbia and Croatia in the 1990s* (Ithaca: Cornell University Press, 2004).

However, at least two other possible motivations for the attacks exist. First, the destruction of Petrokemija – Croatia's leading supplier of agricultural fertilizer – would have profoundly damaged the Croatian agriculture sector.[72] Second, some of the chemicals produced by Petrokemija had military applications. Ammonia, for example, is a key ingredient in many explosives. In short, while the Serbian strikes on Petrokemija may well have been undertaken with the hopes of killing large numbers of non-Serbs living in the area, it seems just as plausible that the strikes were aimed at the Croatian economy and the facility's ability to maintain its critical function as a segment of the Croatian munitions industry.

Following the formal cessation of hostilities in 1995, Croatian officials and chemical industry personnel began an impressive evaluation of "lessons offered" vis-à-vis chemical facility security.[73] In 1996 Petrokemija submitted a report to the United Nations Security Council "recommending that the definition of chemical warfare be changed to include attacks on chemical industries."[74] In 1997 various international chemical industry bodies joined in an effort to understand, prevent, and mitigate chemical "catastrophes triggered or aggravated by combat."[75] Petrokemija now regularly hosts international chemical delegations, providing tours of the plant's facilities with on-hand demonstrations of how the facility was fortified to withstand and respond to military assaults.[76]

In sum, this case illustrates unique attack capabilities and plausible motivations for actual major assaults on a chemical facility. Each putative outcome sought by the Serbs – mass civilian casualties, economic damage or munitions curtailment – ultimately failed. Despite sometimes heavy damage, Petrokemija was operational throughout the war.[77] Given the familiarity Serbian officials had with the target and its environs, and given the variety of effective weaponry employed by the Serbian military to conduct the attacks, these outcomes appear somewhat surprising. They may also demonstrate, however, the important lesson that damaging a chemical facility in a way that produces a catastrophic accident or interrupts key economic processes is difficult, even when intended.

Although few in number, the cases identified in the literature assessment indicate that at least some state and non-state actors recognize the value that certain chemical facilities have as potential targets. The next portion of this section examines in greater detail *why* chemical CI may be particularly valuable targets for terrorists.

---

[72] Croatia's main exports at the time of the war were fruits and vegetables, chemicals**,** iron, steel and textiles. The 1999 NATO strikes on Serbia—operating as part of "Operation Allied Force"—halved that state's economic output via strikes on its oil and chemical industry. Steven Erlanger, "Bombing Unites Serb Army As It Debilitates Economy -- Production Cut in Half, Experts Say," *New York Times*, April 30, 1999, p. A1.

[73] Hostilities between Serbia and Croatia (along with the war in Bosnia) officially ended on December 14, 1995, when leaders of Croatia, Bosnia, and Serbia signed the Dayton peace accords.

[74] Department of Justice, 2000, p. 24.

[75] "Chemical and Biological Medical Treatment Symposium: Croatia, *Applied Science and Analysis Newsletter*, October 1998. <http://www.asanltr.com/ASANews-98/cbmts-indi.html>.

[76] In 1998 a delegation observed Croatian MIG 21s making runs over Petrokemija with mock weapons release. Subsequent to this simulated air attack, the delegation witnessed the Croatian Army deploy its NBC team into the area, followed by medical helicopters swooping in to assist in medical evacuation and treatment of the "wounded." *Ibid*.

[77] Mesaric, telephone interview.

C. Possible Terrorist Objectives for Attacking Chemical CI

Besides presenting a persuasive, albeit anecdotal, case that terrorists are actively interested in targeting chemical CI both in the United States and overseas, the literature assessment indirectly provided important insight into the reasons *why* terrorists might target such facilities. CNS researchers discovered that the majority of literature explicitly addressing terrorism and chemical infrastructure took for granted the notion that terrorists would attack chemical facilities with the primary objective of either: 1) causing massive death and / or destruction; or 2) acquiring chemicals that could later be used to cause massive death and / or destruction. A 2004 Congressional Research Service report, for example, describes the nature of the current terrorism hazards facing chemical facilities with the following language:

> "Potential terrorist acts against chemical facilities might be classified roughly into two categories: direct attacks on facilities or chemicals on site, or efforts to use business contacts, facilities, and materials (e.g., letterhead, telephones, computers, etc.) to gain access to potentially harmful materials. In either case, terrorists may be employees (saboteurs) or outsiders, acting alone or in collaboration with others. In the case of a direct attack, traditional or nontraditional weapons may be employed, including explosives, incendiary devices, firearms, airplanes, computer programs, or weapons of mass destruction (nuclear, radiological, chemical, or biological).
> "In obtaining chemicals a terrorist's intent may be their use as weapons or to make weapons, including but not limited to explosives, incendiaries, poisons, and caustics. Access to chemicals might be gained by physically entering a facility and stealing supplies, or by using legitimate or fraudulent credentials… to order, receive or distribute chemicals."[78]

General descriptions such as this do an adequate job of broadly defining the scope of potential terror attack types that should be considered in policy discussions relating to chemical facility security. They do less well, however, in helping decision-makers understand the more nuanced range of objectives that might motivate terrorists to specifically target chemical CI. Although no single source in the literature assessment identifies all of the following as possible terrorist objectives for critical chemical infrastructure attacks, the literature taken as a whole suggests that terrorists might target chemical infrastructure to accomplish operational objectives that fall into one or more of nine discrete categories. These include: causing human casualties; causing physical destruction; causing environmental contamination; damaging the economy; disrupting strategic industrial functions; acquiring supplies of chemicals; influencing the general public; establishing bargaining leverage for negotiations; and facilitating organization building efforts. A handful of key findings relating to each of these possible objectives are particularly worth noting.

- *Human Casualties.* In 1993 the Office of Technology Assessment estimated that a successful attack on a toxic chemical plant had the potential to cause thousands of fatalities – more than could be expected from any other type of terrorist attack except those involving an efficient, contagious biological agent or the detonation of a nuclear bomb in a major city.[79] Today, it is a widely accepted fact that a successful terrorist strike on a facility – stationary or mobile – containing large quantities of TICs has the potential to result in devastating immediate and long-term human consequences, in terms of deaths, injuries and latent health problems. Just how significant the human toll from such an event might be is extremely difficult to predict. A large number of variables – such as facility location, local population distribution, time of release, atmospheric conditions (including barometric pressure and winds), and quantity and type of chemical released – have the potential to dramatically affect the lethality of a TIC release.

[78] Linda-Jo Schierow, "Chemical Plant Security," Congressional Research Service, January 20, 2004, p.2.
[79] Data from the Office of Technology Assessment, *Proliferation of Weapons of Mass Destruction: Assessing the Risks*, U.S. Congress, 1993 as cited in *Protecting the American Homeland: A Preliminary Analysis*, The Brookings Institution, 2002, p. 6.

A variety of figures are referenced by media and government studies when discussing the potential lethality of terrorist attacks on chemical facilities. Three are most common:

- 41 Million People. In 1998 the US Public Interest Group and National Environmental Law Center issued a study that used 1995 chemical storage information and zip code information to estimate that 41 million Americans – or one out of every six Americans – live in areas where "there could be serious injury or death in the event of a chemical accident created by neighboring industrial facilities."[80]

- 10,000 to More than 1 Million People. Based on EPA statistics presented in Belke's September 2000 study of reported RMP data, a large number of reports on terrorism and chemical CI have reported that: "At least 123 plants each keep amounts of toxic chemical that, if released; could form deadly vapor clouds that would put more than 1 million people in danger… more than 700 plants could put at least 100,000 people at risk, and more than 3,000 facilities have at least 10,000 people nearby.

- 2.4 Million People. Leaked findings from a classified 2001 study conducted by the U.S. Army Surgeon General indicate that a "terrorist attack resulting in a chemical release in a densely populated area could injure or kill as many as 2.4 million people… 'even middle-range casualty estimates from a chemical weapons attack or explosion of a toxic chemical manufacturing plant are as high as 903,400 people.'"[81]

For obvious reasons, such figures do little to provide a clear understanding of how many individuals might be harmed in specific attack scenarios. Three particular qualifications to such figures should be noted. First, most numbers such as these are worst case scenarios that identify the total number of people who work or live within a certain proximity to a chemical facility. In the event of an actual chemical release, only an unfortunate fraction of such a population – those who are in the path of the TIC plume – would be immediately affected. Second, most such figures concern accidents not terrorist attacks. The EPA figures found in Belke's report, in particular, may be misleading in the context of terrorism discussions, because they are based on Clean Air Act RMP information designed to "estimate the effects of a toxic chemical release involving the greatest amount of the toxic chemical held in a single vessel or pipe – not the entire quantity on site."[82] It is highly likely that an intentional terrorist attack on chemical CI would be designed to generate maximum damage – by rupturing multiple vessels or pipes simultaneously, for example – which would in turn release greater quantities of lethal TICs than currently estimated using accidental release information. Finally, it is worth noting that such figures focus on stationary targets only. It should be remembered, however, that mobile chemical CI – such as the 90-ton rail tanks used to store and transport chlorine[83] or the larger ferries and ships that transport chemicals on our waterways – crisscross the nation and jeopardize whatever populations they happen to be close to at a particular time.

---

[80] USPIRG, *Too Close to Home: Chemical Accident Risks in the United States*, 1998, as found at: http://uspirg.org/uspirg.asp?id2=5067&id3=USPIRG&.
[81] Pianin, Eric, "Study assesses risk of attack on chemical plant," *Washington Post*, March 12, 20002, as reported in Schierow, 2004, p. 10.
[82] GAO, 2004, p7.
[83] Although widely used in common industrial processes such as water purification, bleach production, and organic compound manufacturing, chlorine is an example of a highly toxic industrial chemical that is widely stored and used in large quantities across the country. As noted in Thomas Burklow et al., "Industrial Chemicals: Terrorist Weapons of Opportunity," chlorine – which his commonly known as a pulmonary, inhalational, or choking agent – became the "first chemical agent used on a large scale in modern warfare" when, in April 1915, the German Army released 168 tons of chlorine on British troop stationed in Ypres, Belgium. Strikingly, just two contemporary rail tanks hold 180 tons of chlorine.

Regardless of the exact numbers involved, what is absolutely clear is that a successful attack on a critical chemical infrastructure could cause very large numbers of human casualties. Based on open source information, terrorists are certainly aware of this fact too.

- *Physical Destruction*. Although much of the literature relating to critical chemical infrastructure and terrorism focuses on the harm chemicals can cause because of their toxicity, it should be kept in mind that many industrial chemicals are also highly volatile and flammable. Instead of seeking to release toxic chemicals, terrorists have the option of trying to attack chemical facilities in a manner that causes massive explosive reactions and resulting physical damage. Not only would such attacks harm many people, they would also damage surrounding physical assets. One of the most tragic examples of this reality was a catastrophic series of explosions at a propane gas distribution center in Mexico City in 1984. Considered the second most deadly chemical accident in history after Bhopal, the event killed nearly 500, injured 4,000 and leveled 2,000 houses in a 20 block area.[84]

  A 2000 Department of Justice document emphasizes that the objective of causing "massive damage" might be a particularly strong motivation for terrorists to attack chemical facilities, because many sites storing or using large quantities of TICs are also the types of facilities that terrorists have historically sought to destroy, including symbolic and functional targets such as "military installations, federal facilities, and utility companies."[85] Finally, it is plausible to suggest that given the difficulty of predicting outcomes relating to toxic gas releases (due to the uncontrollability of influential factors such prevailing winds and barometric pressure), terrorists might determine that attacking chemical CI in the effort of causing massive explosions is a more reliable form of attack than seeking a TIC release.[86]

- *Environmental Contamination*. A third objective that terrorists might seek from an attack on critical chemical infrastructure is environmental contamination. The release of certain TICs in sufficient quantity can effectively contaminate a locality for decades, causing massive economic damage and community disruption. Strategically approached, such an attack objective might be particularly devastating if launched on a facility in or near a population center, important agricultural region, or symbolically significant location (such as a national park or icon). Analysis by the Department of Justice indicates that nearly 3,000 facilities have reported risk management plans that indicate their potential to significantly affect environmentally important locations in the event of an accidental TIC release.

- *Economic Harm*. As discussed in Section 1, the chemical industry is a "keystone" of the American economy. Tens of thousands of products and services are directly dependent on the industry for its inputs and processes. Terrorists familiar with how certain chemical facilities support the economy, theoretically, could identify particular targets with the specific objective of causing economic harm. Case #11 in Section 3, for example, explains how the destruction of one chemical plant in Texas (the case was ultimately deemed an accident, not a terrorist attack) had a dramatic economic ripple effect, causing $20 million in physical damage, $200 million in lost corporate earnings, noticeable increases in worldwide commodity prices for four significant industrial chemicals, and an increase in consumer gasoline prices in the United States and Europe.[87]

---

[84] Violence Policy Center, 2002, as found at: http://www.vpc.org/studies/ducktwo.htm

[85] Of the RMPs collected by EPA by 2000, 80 were Department of Defense facilities and 15% were infrastructure facilities. The infrastructure facilities included: 1903 water supply and irrigation facilities; 56 electricity generation, transmission or control facilities; and 14 natural gas distribution facilities. See DOJ, 2002, pp. 29-31.

[86] Belke's RMP study notes, for example, that compared with toxic chemical releases that only affect the portion of the population that encounter the plume of TICs carried by prevailing winds, flammable worst-case scenarios "consist of an overpressure blast wave which generally travels in all directions from the source. While terrain and obstructions will affect the propagation of the blast wave to some degree, in general everyone within the worst case circle would feel the effects of a vapor cloud explosion resulting from a flammable substance release."

[87] Specifically, propylene oxide, propylene glycol, methyl tert-butyl ether (MTBE) and styrene.

For the purpose of discussion, it should be noted that the U.S. is the world's largest chemical producer, accounting for 26% of all global production. The conscious targeting of American chemical facilities might actively encourage other nations to become less reliant on the U.S. for essential chemicals, thereby permanently damaging the American economy with the loss of related production jobs and profits.

- *Strategic Function Interruptions.* In the truest sense of "critical infrastructure" attacks, terrorists might seek to destroy certain critical chemical facilities that are sole sources for essential products and services. The identities of such facilities are carefully guarded secrets, and appropriately so. Recent comments by a security specialist associated with the American Chemistry Council, however, provide insight into the type of facility that terrorists might specifically seek to achieve the objective of interrupting strategic functions: "We have one member – a petrochemical plant – that manufactures jet fuel and is the sole supplier for four Air Force Bases… It can be replaced [if destroyed, but] this would take time and the planes would be grounded for that period."[88]

  Even if terrorists don't destroy a chemical CI, if they are successful in releasing TICs they may be able to seriously interrupt strategic functions at the target site. The Justice Department has noted that "a chemical release would be particularly effective at disrupting the operations of strategic sites, even if no off-site consequences resulted. A chemical release may be more effective than a bomb in causing disruption, since a leak of toxic chemicals may necessitate large-scale evacuation."[89] In the same way, terrorists might attack a chemical facility to release TICs with the intent of interrupting strategic functions at locations in the vicinity of the attacked target.

- *Weapon Acquisition*. It has long been suggested that terrorists might attack a nuclear power plant to obtain the fissile material needed for an improvised nuclear device. It is just as conceivable that terrorists might attack a chemical facility with the objective of acquiring industrial chemicals that could be used either independently as chemical agents or as precursors to a weapon. A 2004 CRS report presents a striking real world example of how terrorists may exploit chemical facilities to potentially provide chemical weapons:

  > "[O]ne of the 1993 World Trade Center bombers, Nidal Ayyad… graduated from Rutgers University, and worked as a chemical engineer at Allied Signal, from which he used company stationary to order chemical ingredients to make the bomb… testimony at the trial of the bombers indicated that they had successfully stolen cyanide from a chemical facility and were training to introduce it into the ventilation systems of office buildings."[90]

  If vehicles carrying TICs are considered as a part of the nation's chemical infrastructure, the situation appears particularly vulnerable to terrorist exploitation. Every day tens of thousands of trucks, railcars, barges and ships haul toxic, flammable and explosive chemical cargos around the nation. Such vehicles rarely, if ever, have security. Moreover, if successfully attacked and captured, they can provide terrorists with a ready-made getaway solution that allows for the successful transportation of stolen chemicals.

- *Terrorism Proper.* As discussed in CNS' previous terrorism and critical infrastructure study, terrorism is best understood as violence that is consciously carried out by perpetrators in order to influence the attitudes and behavior of a wider target audience (or multiple target audiences).

---

[88] Kathleen McFall, "Nationwide Chemical Sites Are Targets of Opportunity," December 1, 2003, as found at: http://enr.construction.com.
[89] Department of Justice, 2000, p. 31.
[90] Linda-Jo Schierow, 2004, pp. 4-5.

Terrorists may target chemical CI for the sole objective of influencing the public. In particular, critical chemical infrastructure might be viewed by some terrorists as attractive targets for:

- Generating Publicity. Given that no terrorist group has yet to successfully attack a chemical facility in the United States, it is conceivable that some terrorists might target chemical CI simply to gain the public notoriety for and institutional cache of achieving such a "first."

- Eliciting Fear. A chemical release is sure to cause widespread disruption, panic and fear, even if not ultimately lethal. This is especially likely given that numerous industrial chemicals are also recognized as declared chemical weapons – chlorine and phosgene, for example – and that chemical weapons are recognized as weapons of mass destruction.

- Undermining public confidence in government. As discussed previously, the government has long been aware of security vulnerabilities related to chemical infrastructure. Terrorists might seek to exploit the lack of stronger action by various government institutions (such as Congress and the White House) to regulate chemical facility security, by conducting an attack and hoping that public anger at the consequences would be – at least in part – directed at public officials.

A finding by the Advisory Panel to Assess the Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction summarizes the potential psychological power that an attack on a critical chemical infrastructure might have very clearly, "Terrorism, in essence, is a form of psychological warfare. The ultimate objective is to destroy the structural supports that give society its strength by both showing that the government is unable to fulfill its primary function and, thereby, eliminating solidarity, cooperation, and interdependence on which social cohesion and functioning depend. Viewed in this context, even a "limited" terrorist attack involving [WMD, such as lethal chemicals] would have disproportionately large psychological consequences, generating unprecedented fear and alarm throughout society."[91]

- *Negotiating Tool.* Given the objectives already discussed, it is worth suggesting that terrorists might target chemical infrastructure with intentions other than simply destroying their target or releasing the TICs that it has on site. In particular, terrorists might determine that capturing and holding a chemical facility hostage provides a highly influential form of negotiating leverage, simply because of the potential human, physical, economic, environmental or psychological damage they could threaten while in control of the facility. If the public were aware of such a hostage situation – and particularly if they were aware of the massive potential harm the terrorists could cause if they destroyed the facility or released the TICs it contained – the government would be placed under enormous pressure to successfully diffuse the situation without incident, which might make it more willing to acquiesce to terrorists demands.

- *Organization Building Effort.* Terrorists seeking to strengthen the image and status of their organization vis-à-vis other groups, might attack critical chemical infrastructure specifically because so few attacks have been conducted to date. A successful attack against a chemical target would demonstrate publicly a terrorist group's operational capabilities as well as highlight its willingness to engage in non-traditional means to advance its agenda. It is conceivable that terrorists could try to maximize the appearance of such qualities to boost group morale and bolster recruitment efforts.

[91] Department of Justice, 2000, p. 25.

It is quite likely that terrorists targeting critical chemical infrastructure would seek to attack chemical facilities for more than just one of the nine objectives identified above. Recognizing these objectives as distinct from one another, however, will help analysts and decision-makers remain aware of the broad scope of operational objective motivations that terrorists can have for attacking critical chemical infrastructure. Before concluding this section, three final points should be made about the current nature of chemical facilities and how particular characteristics of such infrastructure might make them particularly attractive as targets to terrorists.

First, as has been discussed repeatedly, certain chemical facilities have the potential of being attacked in order to cause catastrophic damage. Terrorists desiring the capabilities of WMD can sidestep many of the technical and resource hurdles associated with acquiring such weapons by attacking critical chemical infrastructure. Rising global levels of education and the increasing number of individuals who have chemical engineering training suggest that more and more terrorists will have the basic skills necessary to successfully do damage by attacking chemical facilities.

Second, chemical facilities are ubiquitous and often located near population centers and critical transportation hubs. This geographical reality offers terrorists both numerous potential targets to choose from and numerous targets that can have cascading effects if successfully attacked.

And third, most critical chemical infrastructure remains relatively – as compared to other high value targets – ill secured. Despite recognition that chemical facilities can be attacked with catastrophic consequences, little has been done to enhance physical security around most chemical facilities. As mentioned previously, the worst-case scenario for a terrorist attack on a domestic industrial chemical facility calculated by the U.S. Army Surgeon General's Office would result in "up to 2.4 million people killed or injured – close to the number estimated by chemical companies themselves."[92]

In contrast, a worst-case estimate for a successful terrorist attack on a commercial nuclear power plant, specifically a severe pool fire, projects 28,000 cancer fatalities and $59 billion in damage.[93] Yet, while Congress has crafted thorough and effective legislation insuring the security of Nuclear Regulatory Commission (NRC) licensed commercial nuclear power plants, no federal laws explicitly compel chemical facilities to safeguard their facilities against a terrorist attack. The events of 9/11 have done little to change these legislative differences. While the NRC enacted new Orders designed to bolster security at its licensed plants,[94] the chemical industry has been slow to respond and still relies on "voluntary" measures enacted by individual chemical companies in addressing the threat of terrorism.[95]

---

[92] Eric Pianin, "Study assesses risk of attack on chemical plant," *Washington Post*, 12 March 2002.

[93] These figures were calculated in a 1997 report for the NRC by Brookhaven National Laboratory. As reported in. Robert Alvarez, "What About the Spent Fuel?" *Bulletin of the Atomic Scientists*, January/February 2002, p.46.

[92] See, Dr. Richard A. Meserve, Chairman, Nuclear Regulatory Commission, "Statement Submitted by the United States Nuclear Regulatory Commission to the Committee on Environment and Public Works, United States Senate, Concerning Power Plant Security," 5 June, 2002.

[93] It should be noted that legislation was drafted by Senator John Corzine (D-NJ) that would have required chemical companies to identify their vulnerabilities via-a-vis terrorists and organize security plans to address them. After intense governmental debate, which included lobbying by the chemical industries trade associations, the Senate passed the Chemical Security Act of 2003. This bill, however, was "substantially revised" and continues the trend of voluntary implementation of security measures by the chemical industry. For the full text of the Chemical Security Act of 2003—S.157—see: http://thomas.loc.gov.

Section 3

CrITIC CHEMICAL INFRASTRUCTURE CASES

A. Critical Infrastructure Terrorism Incident Catalog

As part of the research effort associated with its August 2004 study of terrorist motivations for attacking critical infrastructure, 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.

B. CrITIC Methodology

CrITIC was originally designed to offer researchers a tool that would enable them to examine data related to critical infrastructure attacks in a quantitative and systematic manner. To facilitate this endeavor, CrITIC was designed to capture information from terrorist incidents involving critical infrastructure in eighteen discrete fields. (See Figure 3.1.) To be included in the database, incidents had to meet the following five criteria:

1) incidents had to involve an actual attack – planned and preempted attacks were not included in the database (mainly for reasons of consistency and lack of sufficient information[96]); and

2) incidents had to be conducted by a violent non-state actor(s) in a non-combat environment – attacks against CI conducted by states or parties involved in civil war were not considered terrorist acts; and

3) incidents had to have an identifiable impact on critical infrastructure (intentionally or inadvertently); or

4) incidents had to have a significant and identifiable potential of having an impact on critical infrastructure (either intentionally or inadvertently) even if they did not result in such; or

5) perpetrator(s) had to intend for the incidents to have a major impact on critical infrastructure.

Because existing open sources are unable to provide a representative sample of cyber-attacks, and because such attacks involve a different set of issues requiring analysis, cyber attacks against critical infrastructure were not recorded in the database.[97] (A detailed explanation of the CrITIC methodology can be found in Chapter 4 of CNS' August 2004 study on pages 86-95.)

---

[96] It should be noted that CNS researchers did identify one actual case that, due to lack of information, was not included in the following case studies. In a 2000 report, the Department of Justice identified that members of the Revolutionary Armed Force of Columbia (FARC), "blew up a pesticides warehouse in Une, Columbia, resulting in large volumes of toxic materials being released into the air." The attack, according to the DOJ, caused the evacuation of 9,000 people "to prevent mass poisoning from the toxic emissions." Subsequent research by CNS has revealed no other open-source documentation of this incident.

[97] Where cyber-based attacks had physical effects on a physical infrastructure, the incident was recorded under the category of the physical infrastructure.

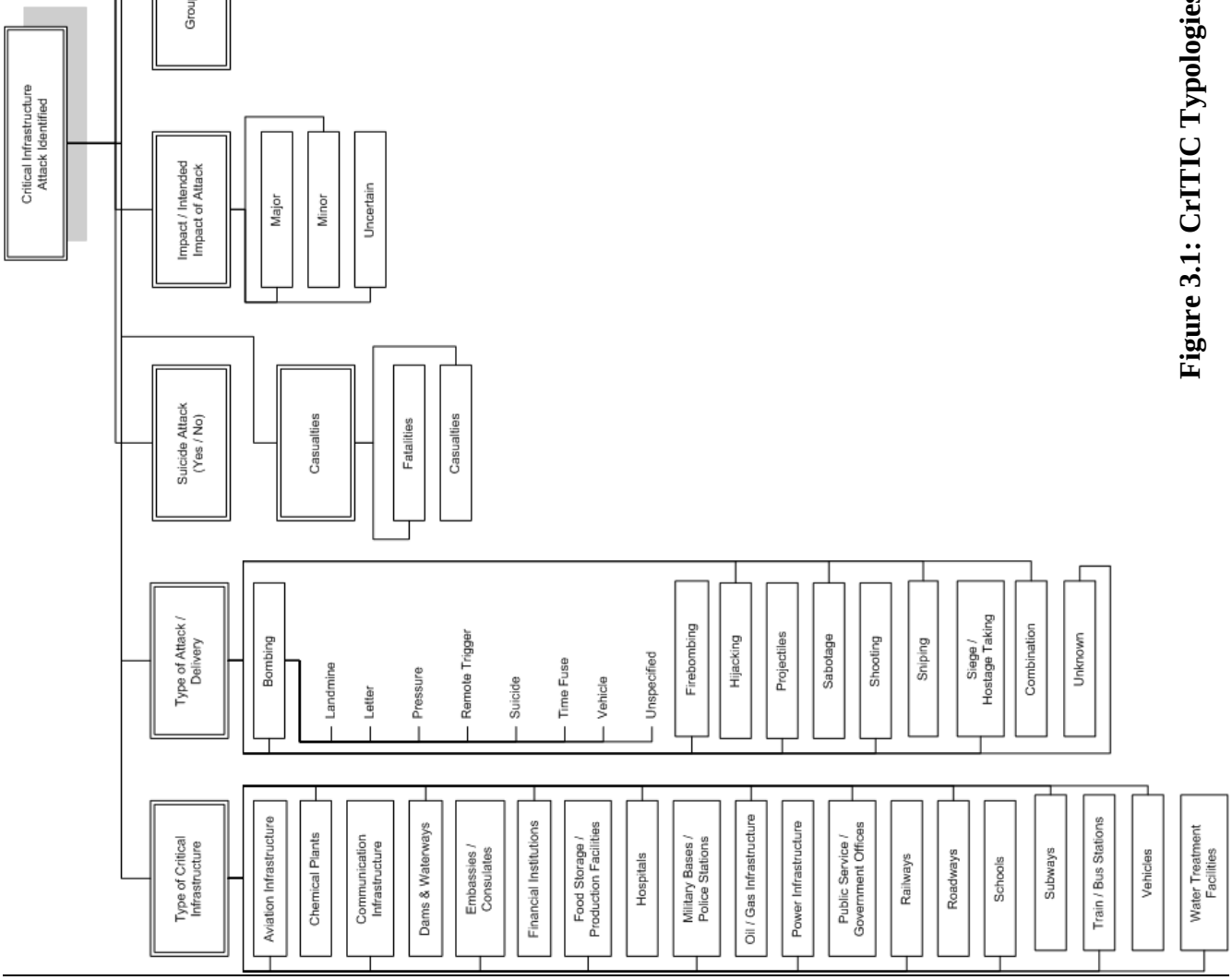


Figure 3.1: CrITIC Typologies

Perpetrators / Year	Motivation/Objective	Ideology	Target / Location	Tactic	Delivery	Outcome
MLN/Tupamaros (1965)	Demonstrate anti-US sentiment	Leftist	Bayer A.G. Facility Uruguay	Bomb	Unknown	None specified
People's Resistance Army (1974)	Protest U.S. support of Greek government	Leftist	Dow Plastics Plant Lavrion, Greece.	5 Bombs	Planted in facility	Two killed; unknown number of injuries
Shining Path (1983)	Anti-government; anti-US sentiment	Leftist	Bayer A.G. Plastics Plant Lima, Peru	Bombs	Planted in facility	$30 million in property damages; no specific number of fatalities or casualties
Unknown (1984)	Probable Accident / Possible Sabotage	Unknown	Union Carb Pesticide Plant Bhopal, India	Gas Leak	NA	Thousands of deaths and injuries
Peace Conquerors (1985)	Protest corporate environmental practices and policies; anti-US sentiment	Eco-Radical	Bayer A.G. Brussels HQ Brussels, Belgium	Bomb	Placed in a mailbox adjacent to Bayer headquarters	Property damage
Peace Conquerors (1985)	Revenge for 1984 Bhopal accident; protest military policies	Eco-Radical	Union Carb. Battery Plant Rosebury, Australia	Bomb	Placed in facility	Property damage
Red Army Faction – Suspected (1986)	Unknown	Leftist	Bayer A.G. Chemical Plant Cologne, West Germany	2 Bombs	Unknown	None specified
Red Army Faction – Suspected (1989)	Unknown	Leftist	Bayer Research Center Düsseldorf, West Germany	Bomb	Unknown	Bombs deactivated before exploding
Middle Eastern Islamic Liberation Front (ILF) – Claim Only (1990)	Probable Accident / ILF claim: to protest US support of Israel; hinder US defense production	Anti-American / Anti-Israeli	ARCO MTBE Facility Channelview, Texas	Explosion	NA	Widespread property damage; seventeen deaths and five injuries; explosion due to accident, not terrorism
Unknown (2004)	Anti-American; anti-West	Religious (Islamist)	ABB Lummas Global Inc (Representative Target) Saudi Arabia	Firearms	Gunmen	U.S. ambassador to Saudi Arabia urging Americans to "Go home. We cannot protect you"

Table 3.1: Summary of CrITIC Chemical Infrastructure Attacks

Case 1

Location: Unspecified location, Uruguay

Date: 9 August 1965

Perpetrator: Movement of National Liberation (MLN: Movimiento de Liberación Nacional); also known as the Tupamaros[98]

Target: Bayer A.G. Facility (Possibly a Warehouse)

Tactic: Bombing

Motive: Demonstrate anti-U.S. sentiment

Incident Description: The MLN, or Tupamaros, was responsible for the bombing of a facility, possibly a warehouse, owned by the West German chemical and pharmaceutical company Bayer A.G.[99] There were no reported deaths or injuries, although this may simply have been due to the remote, non-urban location of this facility. There is no indication that this was a suicide attack.

The Tupamaros, a leftist political group, grew out of the student protests against the repressive, right-wing government. Although it initially cultivated a "Robin Hood" image, the group became increasingly violent over time, even targeting foreign diplomats and businessmen for kidnapping and assassinating policemen. A large protest against U.S. military involvement in Southeast Asia has been suggested as the precipitant of the August 1965 attack on the Bayer facility. Although specific connections between Bayer and the U.S. military are tenuous, the attack may have been launched in response to allegations of the company's involvement in manufacturing products used by the U.S. Army.

[98] The name "Tupamaros" is derived from condensing the name of a historical Peruvian Inca, Tupac Amarú, who led an uprising against colonial Spaniards and thereby achieved semi-legendary status in parts of South America. The same name is also linked to another left-wing political group in South America – the Tupac Amura Revolutionary Movement (MRTA) of Peru. There is no indication that the Uruguayan group had any specific influence on or link with the Peruvian group.

[99] Charles A Russell and Robert E Hildner, "The Urban Guerrilla in Latin America," *Air University Review*, September-October 1973, accessed 20 July 2004, <http://www.airpower.maxwell.af.mil/airchronicles/aureview/1973/sep-oct/russell.html>.

Case 2

Location: Lavrion, Greece

Date: 23 February 1974

Perpetrator: People's Resistance Army (or Popular Resistance Army); also known as Laos-8

Target: Dow Chemical Plastics Production Facility

Tactic: Multiple Bombs

Motive: Protest U.S. support of Greek government

Incident Description: A Dow Chemical facility was damaged after the unexpected detonation of a bomb on the premises during an attempt to defuse it.[100,101] After five bombs were reportedly found at their plastics production plant, Greek demolition experts were dispatched to the Lavrion (also identified as Laurion or Laurium) facility near Athens. It is unclear from reports whether all five bombs detonated, one while a bomb-response team was working on it,[102] or if only one bomb exploded during efforts to defuse it.[103] At least two of the bomb disposal experts were killed in the blast, and an unknown number may have been injured.

Responsibility for the attack was claimed by the People's Resistance Army,[104] alternatively identified as the Popular Resistance Army,[105] via anonymous phone calls to news agencies. Available open-source literature asserts that this group was also known by its Greek initials, Laos-8. It has been suggested that this was most likely a mis-identification of the left-wing group Epanastatikos Laikos Agonas (ELA: Revolutionary People's Struggle or Revolutionary Popular Struggle), which had professed similar intentions. Laos-8 may also have been a subset of ELA, or perhaps even a very short-lived group that was either absorbed by or splintered from ELA.[106]

In December 1974, the so-called "Laos-8" group claimed responsibility for car bombings targeting Americans.[107] Their stated motive for those terrorist attacks was to protest the U.S. government's support for the oppressive military regime led by General Dimitrios Ioannides,[108] who had replaced Colonel George Papadopoulos as junta chief in November 1973. Ioannides' government collapsed in July 1974, which may account for the subsequent demise of Laos-8. It was a very unstable time in modern Greek history, during which civil liberties were erratically suspended and marginally restored, and many opponents of the right-wing military junta were imprisoned and tortured.

Case 3

Location: Lima, Peru

---

[100] Edward F. Mickolus, *Transnational Terrorism: A Chronology of Events, 1968-1979* (Westport, CT: Greenwood Press, 1980).
[101] Information Bank Abstracts, *New York Times*, 24 February 1974, Sunday, p. 7.
[102] Mickolus, 1980.
[103] Information Bank Abstracts, *New York Times.*
[104] Mickolus, 1980.
[105] Information Bank Abstracts, *New York Times.*
[106] Personal Communication with Dr. Jeffrey Bale, September 9, 2004.
[107] Mickolus, 1980.
[108] Mickolus, 1980.

Date: 27 May 1983

Perpetrator: Sundero Luminoso (SL: Shining Path) – Suspected

Target: Bayer A.G. Plastics Production Facility

Tactic: Multiple Bombs or Incendiary Device

Motive: Anti-government and anti-U.S. sentiment

After a series of bombings in Lima, Shining Path guerrillas were believed to have been responsible for an attack on a chemical plant owned by the Bayer Corporation.[109] The incident occurred simultaneously with other attacks in the Peruvian capital that were aimed at disrupting the overall infrastructure. Along with their industrial chemical facility, electricity towers, a water treatment facility, a well-traveled bridge, the U.S. Embassy, the presidential palace, and a bank were also targeted.[110] (The successful attack against the electricity towers left Lima powerless for hours.) Shining Path activity had previously focused on rural central Andean regions of Peru and this attack had been cited as the first major incursion into an urban setting. It appears as if the plant was merely one opportunistic target among many in a wider campaign against infrastructure.

In coordination with other guerrillas around the city, twenty armed members of the Shining Path allegedly invaded the Bayer plastics plant after dark.[111] At least three explosions were reported at the industrial chemical facility. Whether three bombs were detonated or a single incendiary device generated multiple explosions is not clear. The plant sustained heavy damage[112] estimated at $30 million.[113] No specific number of fatalities or casualties was reported. Although it did not officially claim responsibility for the attack at that time, all the evidence points to the group. Shining Path, a violent offshoot of the Partido Comunista del Peru (PCP: Communist Party of Peru), is an indigenous, insurgent group whose proclaimed motivation is to overthrow the government and implement a Maoist-style communist system by violent revolutionary means. The U.S. State Department considers Shining Path to be a terrorist organization, as do the majority of Peruvians.

---

[109] "Dynamite attacks plunge Lima into darkness," *United Press International (UPI)*, 27 May 1983.
[110] Michael R. Meyer and Michael Smith, "Peru: the 'Shining Path' to terror," *Newsweek*, 13 June 1983, p. 33.
[111] "Bayer's plant resumes after terrorist attack," *Chemical Week*, 29 June 1983, p. 14.
[112] Reuters, "Police detain 500 in Peru bombings," *New York Times*, 30 May 1983.
[113] Edward F. Mickolus, Todd Sandler, Jean M. Murdock, *International Terrorism in the 1980's: A Chronology of Events*, vol. 1, 1980-1983, (Ames: Iowa State University Press, 1989).

The attacks on infrastructure by Shining Path were intended to disrupt the functioning of the government. In this case, the chemical plant was probably targeted because of the ruling regime's ties to western capitalist governments, in particular the U.S. government – "in the cities, they attacked Yankee imperialism directly, striking at the Bayer chemical plant in Lima."[114] Bayer is not a U.S. company, but it was seen as being symbolically affiliated with the U.S. The success of the overall attack that Friday night in May 1983 was later used by Shining Path and its supporters as a rallying point marking the "beginning of the People's War."[115]

[114] "Why the People's War in Peru is Justified and Why it is the Road to Liberation," text of speech by Heriberto Ocasio (National Spokesman Committee to Support the Revolution in Peru, Berkeley CA), May 1995, <http://www.csrp.org/15year.htm>.
[115] *Ibid*

Cases 4 and 5

Location: Düsseldorf (Case 4) and Cologne (Case 5), West Germany

Date: 29 April 1985 (Case 4) and 3 May 1985 (Case 5)

Perpetrator: Revolutionäre Zellen (RZ: Revolutionary Cells)

Target: Hoechst A.G. Office Buildings

Tactic: Bombs

Motive: Protest perceived German economic imperialism

Incident Description: To protest the approaching G7 economic summit meeting in Bonn, a leftist group detonated multiple bombs at office buildings housing major German business and banking industries. Two of these targeted a major West German chemical and pharmaceutical company.

On 29 April 1985, at the start of the work week, a bomb was detonated in front of the offices belonging to Hoechst A.G. (which merged with the French company Rhône-Poulenc in December 1999, forming Aventis, now headquartered in Strasbourg).[116] Two other bombs were placed at a Deutsche Bank-affiliated structure in Cologne, and at the headquarters of an aerospace industry trade organization in an unspecified location near Bonn. Four days later, in the same calendar week, a bomb exploded along an outer wall of a building occupied by a French subsidiary of Hoechst in the city of Cologne, approximately twelve miles northwest of Bonn.[117] Property damage to the Hoechst office was initially estimated at $17,000. Another, larger bomb was disarmed before it detonated in the courtyard of the main West German defense contractor, the Defense Technical Procurement Agency in Koblenz. No fatalities or casualties were reported in any of these incidents. Both of the Hoechst-affiliated targets were administrative office buildings, not industrial chemical production facilities.

Letters were sent to multiple local German newspapers in which responsibility for the blasts was claimed by a radical leftist group known as the Revolutionäre Zellen. The RZ is reported to have had connections with another prominent violent leftist group, the Rote Armee Fraktion.

The letters claimed that those bombings were meant to protest "the plundering of the Third World by West German banking and business concerns."[118] They were timed to coincide with the arrival of leaders from the seven major economic powers of the world for the annual economic summit. The RZ had also expressed its opposition to those systems responsible for "inhuman technocracy,"[119] which a major chemical and biotechnology company could easily be characterized as by a radical Communist organization.

It should be noted that all of the targets were office buildings, where those who controlled these companies rather than the "workers" were housed. There is no evidence to suggest that there was any danger of a large chemical incident, although there is always the possibility that a future attack directed against the management/owners of a chemical facility could have the unintended consequence of a toxic chemical release.

---

[116] William Drozdiak, "Bombs hit W. German targets: Leftists say attacks linked to summit," *Washington Post*, 30 April 1985.
[117] Joseph B. Fleming, "Terrorist bombs planted at West German offices," *United Press International (UPI)*, 3 May 1985.
[118] Drozdiak, "Bombs hit W. German targets: Leftists say attacks linked to summit."
[119] Chris Brice, "Terrorism has become the new boom industry," *Courier-Mail (Brisbane, Australia)*, 28 June 1985.

Case 6

Location: Brussels, Belgium

Date: 29 June 1985

Perpetrator: Peace Conquerors

Target: Bayer A.G. Brussels Headquarters

Tactic: Bomb

Motive: Protest corporate environmental practices and policies; anti-U.S. sentiment

Incident Description: A bomb exploded in a mail box adjacent to the Brussels headquarters of Bayer A.G., a major West German chemical and pharmaceutical company.[120] The explosion reportedly produced "little damage," primarily impacting part of the seven-story building's entrance hall and breaking windows on the ground floor.[121,122] No injuries were reported.

Telephone calls were made and letters were sent to major print and radio news services by a previously unknown leftist, ecologically-motivated group called the Peace Conquerors. Their motivation for targeting Bayer was to protest the firm's dumping of chemicals (called "chemical waste" by the group[123]) into the North Sea and to express disapproval about the company's legal actions against Greenpeace, an international environmental nongovernmental organization.[124] The group also proclaimed its opposition to "U.S. militarism," the proliferation of nuclear weapons, and the policies of then-President Ronald Reagan.[125]

Additionally, this group was opposed to airplanes and airport development. The Peace Conquerors had claimed responsibility for the bombing of the Frankfurt Airport three days earlier.[126,127] In that incident, three people were killed and forty-two were injured.[128] The group's threats included mention of targeting more buildings and commercial airplanes. The Peace Conquerors also claimed responsibility for the bomb planted aboard an Air India Boeing 747 jet, which led to its downing off the coast of Ireland and resulted in 329 deaths.[129] The group's rhetoric signaled its intent to escalate its terrorist activity without regard for human life.

While their claims regarding the airport and airplane bombings have been contested, no other group made declarations of responsibility for the Bayer or Union Carbide (see case #7 below) attacks. Nor have the authorities offered any alternative suspects or explanations.

---

[120] "Bomb damages Bayer building," *Associated Press*, 22 June 1985.
[121] "Police say they are taking seriously claim by 'Peace Conquerors'," *Associated Press*, 24 June 1985.
[122] 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, 1980-1983.
[123] "Bomb damages Bayer building," *Associated Press*.
[124] Greenpeace denied any links with the Peace Conquerors.
[125] "New bomb threats by 'Peace' group," *The Telegraph (Sydney, Australia)*, 26 June 1985.
[126] "Police say they are taking seriously claim by 'Peace Conquerors'," *Associated Press.*
[127] Chris Brice, "Terrorism has become the new boom industry," *Courier-Mail (Brisbane, Australia)*, 28 June 1985.
[128] It should be noted that at least six groups initially claimed responsibility for the Frankfurt Germany airport bombing. All six declarations were dismissed by West German investigators. The actual perpetrator is not known.
[129] "Econuts bomb two jets," *The Telegraph (Sydney, Australia)*, 24 June 1985.

Case 7

Location: Rosebury, Australia

Date: 5 July 1985

Perpetrator: Peace Conquerors

Target: Union Carbide Battery Manufacturing Plant

Tactic: Bomb

Motive: Revenge for 1984 Bhopal, India chemical accident; protest military and nuclear policies

Incident Description: The responsibility for a bomb that exploded outside a Union Carbide facility, which assembled flashlight batteries, was claimed by a violent environmental group, the Peace Conquerors, which previously had only been active in Europe.[130,131] The blast reportedly resulted in shattered windows at both the factory and in nearby residential homes. Another report described the damage as much more minimal: "the damage was slight … some windows were broken and a side wall had scorch marks."[132]

The group's stated motivation for this bombing was to exact revenge or retribution for the "collective murder" of those killed in the December 1984 Bhopal disaster. The initial choice of a Union Carbide facility suggests that the group's targeting was symbolic in nature rather than intended to disrupt critical infrastructure in either Europe or Australia. Threats had been made against both the Union Carbide assembly facility in Rosebury and the Union Carbide chemical production plant in Rhodes (approximately ten miles west of Sydney) by an unidentified group six months prior[133] and six days after the Bhopal disaster. Both of those targets are working facilities; Union Carbide's administrative headquarters in Sydney was not reported as a target. This may be an indication that one of the objectives of the attack was to disrupt the functioning of the plant.

The claims also indicated the group's intent to pursue other targets as part of a "campaign for a nuclear free Pacific."[134] Citing Australian and New Zealand support for U.S. and French nuclear testing activities, the Peace Conquerors specifically protested against the deleterious impact these activities have had on Pacific Islanders, especially those indigenous to the tiny island nations near nuclear test sites. The presence of U.S. military troops on Australian territory was also among its stated grievances. While this particular incident did not result in any deaths or injuries, the group reportedly threatened to engage in terrorist activities resulting in the loss of human life if its demands were not heeded.

It should be noted that very few references to this terrorist group are readily accessible in the open literature. The small number of incidents at two disparate geographical locations within three weeks of each other suggests that the Peace Conquerors consisted of a limited number of individuals, perhaps only one Australian who traveled to northern Europe or had ties there. Others have speculated that "this group was local and had a very

---

[130] S. O'Conner, "No threat before factory bombing," *The Telegraph (Sydney, Australia),* 5 July 1985.
[131] "Terror group in Australia?" *The Telegraph (Sydney, Australia),* 9 July 1985.
[132] "Blast at Union Carbide," *The Courier-Mail (Brisbane, Australia),* 6 July 1983.
[133] "Sydney plants threatened," *The New York Times,* 9 December 1984.
[134] "Terror group in Australia?"

short life cycle."[135] The brief duration of this "group" may be suggestive of one or two individuals lacking either firm commitment or financial support for terrorism as a means to escalate their pursuit of a socio-political cause.

It should be noted as well that the first Peace Conquerors incident (case #6) occurred less than two months after the RZ's building bombings in northern Europe, including small-scale attacks on two chemical company administrative offices (cases #4 and #5), to protest the convening of a large western economic summit. The motives and ideologies of the group claiming responsibility for cases #4 and #5, while not exactly duplicated by the Peace Conquerors, reflect similar underlying beliefs. One might also speculate that case #6, the mail-box bombing of the Brussels Bayer office, may also have been inspired by the activities of the RZ, i.e., that it was a "copy-cat" incident.

[135] Personal communication with Dr Jeffrey Bale and Kevin Coogan.

Case 8

Location: Cologne, West Germany

Date: 1 October 1986

Perpetrator: Rote Armee Fraktion (RAF: Red Army Faction) – Suspected

Target: Bayer A.G. Unspecified Chemical Facility

Tactic: Multiple Bombs

Motive: Unknown

Incident Description: Two bombs exploded at a Bayer chemical subsidiary near or in Cologne, West Germany.[136] No injuries were reported. West German police allege a Red Army Faction connection. Nothing was reported relating to the specific motivation for targeting the Bayer facility, nor was the specific type of facility mentioned. The Bayer Corporation is known to have had an administrative office complex in the Cologne area during this time, as well as having had a facility north of the Cologne area.

[136] "Cologne bombing," *The Financial Times (London)*, 1 October 1986.

Case 9

Location: Düsseldorf, West Germany

Date: 12 December 1989

Perpetrator: Rote Armee Fraktion – Suspected

Target: Bayer A.G. Pharmaceutical Research Center

Tactic: Bomb

Motive: Unknown

Incident Description: A small bomb targeting a Bayer chemical facility in Düsseldorf was intercepted and deactivated before exploding.[137] The targeted facility did not engage in chemical production, but was instead a chemical and pharmaceutical research center. Only small-scale laboratory synthesis was done at the location.

A note claiming responsibility and intended for news agencies was found "in the street by a passerby," and this lead to the discovery of a six pound explosive device. The Red Army Faction, a radical Marxist group, was suspected of responsibility. No specific motive was reported, although if the RAF was responsible, the motive was likely to have been similar to that discussed previously in cases 4 and 5.

[137] "West German bomb attack foiled," *The Washington Post*, 12 December 1989.

Case 10

Location: Bhopal, India

Date: 3 December 1984

Perpetrator: Probable Accident; Possible Disgruntled Employee

Target: Union Carbide Pesticide Production Facility

Tactic: Probable Accident / Possible Sabotage

Motive: Unknown

Incident Description: A gas leak at a Union Carbide plant in Bhopal, India, killed approximately four thousand people initially and another three to four thousand in the following weeks; twenty years later, over 14,000 deaths have been linked to the incident, according to official accounts.[138,139,140,141,142] Other estimates suggest a figure closer to eight thousand immediate deaths and more than 30,000 directly linked fatalities in the ensuing years.[143] Casualty figures are in the hundreds of thousands, even by conservative estimates.[144] The repercussions and long-term effects are still being felt.[145]

Bhopal, located approximately three hundred miles south of New Delhi, produced the pesticide Sevin™ from methyl isocyanate (MIC). Used widely in preparing insecticides, methyl isocyanate was first manufactured commercially in the U.S. in the 1960s.[146] The synthesis of Sevin™ involves multiple toxic chemical precursors. Chlorine is first reacted with carbon monoxide to form phosgene; the next step involves the reaction of phosgene with malodorous and corrosive monomethylamine (MMA) to generate MIC. Sevin™ is a carbamate[147] compound produced by reacting MIC with 1-naphthol (α-naphthol), a severe irritant that targets the kidneys.

Arguments continue to this day over the cause of the leak. Union Carbide contends that over one thousand liters of water had been unaccountably introduced into a storage tank holding methyl isocyanate, most likely by a disgruntled employee, thereby precipitating the incident.[148,149] Representatives of the company maintain that

---

[138] Barbara Crossette, "Bhopal's tragedy revisited; 10 years after the gas," *The New York Times*, 11 December 1994.
[139] Dominique LaPierre and Javier Moro, *Five Past Midnight: The Epic Story of the World's Deadliest Industrial Accident* (New York: Warner Books, 2002).
[140] Debora MacKenzie, "Fresh evidence on Bhopal disaster: Documents suggest U.S. company was responsible for plant's design and cut investment to maintain control," *The New Scientist*, 7 December 2002, p. 6, <www.NewScientist.com>.
[141] Mazhar Ullah, "Court refuses to reduce murder charge against Bhopal chief," *The Guardian (London)*, 29 August 2002, <www.guardian.co.uk>.
[142] Marc S. Reisch, "Twenty years after Bhopal," *Chemical & Engineering News*, 82 (23), 7 June 2004. pp. 19-23.
[143] Penny Wark, "The toxic legacy of the explosion of a pesticide factory in Bhopal is still felt 20 years on," *The Times (London)*, 25 May 2004.
[144] Scott Baldauf, "Bhopal gas tragedy lives on, 20 years later," *The Christian Science Monitor (Boston, MA)*, 4 May 2004.
[145] Substantial time and effort can be invested in attempts to resolve and reconcile the differences between the official and unofficial fatality and injury estimates. Due to the socio-economic status of the people living in the area surrounding the Union Carbide Bhopal plant, an exact figure will never be known with certainty. Regardless of the arguments about casualties and causes, the larger figures are now part of the public discourse and, thus, have a chilling and potentially fear-engendering impact on the general populace. Larger figures may also appeal to and empower terrorist types motivated to pursue mass-impact or mass-casualty events.
[146] "Methyl isocyanate: How it is made," *Chemical Week*, 19 December 1984, p. 35.
[147] Carbamates are a class of pesticides distinct from organophosphates; the former are the salts or esters of carbamic acid, $H_2NC(=O)OH$ and do not contain phosphorous, as organophosphates do.
[148] "Bhopal methyl isocyanate investigation team report," Union Carbide Corporation, Danbury, Connecticut, March 1985.

sabotage was the cause of the incident. A highly regarded investigation commissioned by the Indian government and executed by the Arthur D. Little Company[150] concluded that the incident was caused by the connection of a rubber hose directly to the MIC storage tank and the subsequent introduction of a large volume of water.[151,152] When an increase in pressure was noted and the hose was found by plant employees, an attempt was apparently made to transfer some of the tank's contents. It was during this procedure that the methyl isocyanate release reportedly occurred.

Others maintain that the MIC release was the result of a tragic accident in which Union Carbide bears some portion of the blame for its less-than-adequate safety measures. A U.S. Chemical Safety and Hazard Investigation Board (CSHIB) report concluded that "pressurized methyl isocyanate burst through safety valves" of the storage tank due to rapid exothermic polymerization of the MIC.[153,154] It was determined that a critical part of the cooling system was nonfunctional and that, furthermore, a high tank temperature alarm had been disconnected.

In 1989 Union Carbide agreed to pay a $470 million settlement for liability claims. Bhopal is still discussed as a model case concerning the need for vulnerability reduction.[155,156,157]

---

[149] Jackson B. Browning, "Union Carbide: Disaster at Bhopal," 1993, <www.bhopal.com/pdfs/browning.pdf>. Originally appeared in *Crisis Response: Inside Stories on Managing Under Siege*, Jack A. Gottschalk, ed., Visible Ink Press, Detroit, MI.

[150] In the text of the Arthur D. Little report, the author acknowledges that he "and the organization he represents were a part of [the initial Union Carbide Corporation] investigation team." While the Little report was independently commissioned, the author and his organization are not completely disconnected from Union Carbide.

[151] Ashok S. Kalelkar, "Investigation of large-magnitude incidents: Bhopal as a case study," presented at the Institution of Chemical engineers Conference on Preventing Major Chemical Accidents, London England, May 1998, <www.bhopal.com/pdfs/casestdy.pdf>.

[152] Exothermic polymerization of the methyl isocyanate (MIC) in the storage tank had been inhibited by added phosgene, as a minority component of the mixture. Enough water entered the tank to completely react with the phosgene. This in turn led to a build up of carbon dioxide gas that raised the temperature of the MIC. As the temperature in the storage tank increased and the concentration of phosgene decreased, the heat generated by the exothermic polymerization of the MIC occurred at a rate more rapid than the heat could be dissipated, eventually leading the temperature of the tanks contents to skyrocket, i.e., produce a "runaway" reaction. The elevated temperatures caused the MIC to boil violently inducing a huge pressure increase on the external walls and fixtures of the storage tank. Runaway reactions have also been responsible for catastrophic chemical accidents in Sveso, Italy (1976); Lodi, New Jersey (1995); and Paterson, New Jersey (1998).

[153] U.S. Chemical Safety and Hazard Investigation Board, "Hazard Investigation: Improving Reactive Hazard Management," Report No. 2001-01-H, October 2002.

[154] See footnote 61 for explanation of a rapid exothermic polymerization.

[155] Peter Avis, "Planned chemical plant stirs hopes and old fears in India," *The Toronto Star*, 4 February 1995.

[156] Faezah Ismail, "Our responsibility to the future," *New Straits Times (Malaysia)*, 24 January 1995.

[157] Peter Kammerer, "Dead men walking at work every day," *South China Morning Post*, 2 May 2004.

Case 11

Location: Channelview, Texas

Date: 5 July 1990

Perpetrator: Middle Eastern Islamic Liberation Front (ILF) -- Claimed Responsibility Only

Target: ARCO MTBE Production Facility

Tactic: Probable Accident

Motive: Claim: protest of U.S. support of Israel; hinder U.S. defense production

Incident Description: The greater Houston area of Texas has one of the largest concentrations of chemical facilities in the world. In 1990, 46% of the country's major chemicals originated in southeast Texas chemical facilities. On the night of July 5, an explosion at the Atlantic Richfield Chemical Company's (ARCO) Channelview production facility generated a fireball and a blast that was heard ten miles away.[158] While having a dramatic start, the fire was extinguished within four hours. There was no evacuation of people living in the area. The accident, however, did result in seventeen deaths and five injuries to plant workers. In addition to plant damage, the explosion broke windows in residential homes adjacent to the plant.

The Channelview plant, located twenty miles east of Houston, produced raw materials used in the production of a wide variety of consumer goods, such as insulation, packaging materials, automotive and medical parts, and cleaning compounds. Monetary losses due to property damage were estimated to exceed $20 million, and projections for lost business to ARCO hovered around $200 million.[159] The plant's shut-down impacted commodity prices across the worldwide chemical industry for propylene oxide, propylene glycol, methyl tert-butyl ether (MTBE) and, most seriously, styrene.[160] Prices for the latter were reported to leap 30-40% in the incident's wake. The explosive fire was also credited for an increase in consumer gasoline prices in both the U.S. and Europe.[161,162] At the time, MTBE was used as an octane-boosting replacement for lead in motor vehicle fuel. Additionally, ARCO agreed to pay a $3.48 million fine for "willful" violations of federal safety law.[163] A year later, Phillips Petroleum Company was fined $4 million for similar violations that contributed to a 1989 accident at another Houston area chemical production facility, in which twenty-three workers were killed and over one hundred injured.[164] Such accidents have considerable financial impact, in addition to the tragedy of worker fatalities.

Eight days after the explosion, a statement was made by a group identifying itself as the Middle Eastern Islamic Liberation Front (ILF), which claimed responsibility for the incident.[165] The alleged motivation for the attack was

---

[158] David Maraniss, "Texas chemical plant blast kills 17," *The Washington Post,* 7 July 1990.
[159] Simon Reyonolds, "The price of tragedy rises - Industrial risk rates are out of step with the new size of losses," *Financial Times (London),* 9 September 1991.
[160] Andrew Wood and Shelina Shariff, "Fallout from Channelview explosion keeps on coming," *Chemical Week,* 24 June 1990, p. 9.
[161] "ARCO Petrokemijal unit blast jolts markets," *Oil & Gas Journal,* 16 July 1990, p. 28.
[162] Ian Young and Shelina Shariff, "MTBE still leading the way in global octane surge," *Chemical Week,* 18 July 1990, p.16.
[163] Frank Swoboda, "Settlement set in '90 plant blast," *The Washington Post,* 4 January 1991.
[164] "Phillips to pay $4 million for fatal safety violations: 23 workers died in chemical plant blast," *Atlanta Journal and Constitution (Georgia),* 23 August 1991.
[165] "Sabotage? US dismisses ARCO explosion claim," *St. Louis Post-Dispatch (Missouri),* 14 July 1990. Their name is identical to the English version of the well-known international Islamist group, Hizb al–Tahrir al-Islami (HT: Islamic Liberation Front), but it probably purely coincidental.

in response to U.S. support for Israel against the Palestinians. An ILF spokesman was quoted as saying that the ARCO Channelview facility was targeted because "[t]his factory was providing the U.S. Army with chemical equipment, although it was publicly operating as a factory manufacturing supplies for civilians." [166] The claimant continued by asserting that Washington ignores “the human rights of our Palestinian people" and Israeli "killings and terrorism against Palestinian families" in the occupied West Bank and Gaza Strip. "We want Washington to taste the pain of the deaths of its people the same way we feel the pain of the killings of our Palestinian families at the hands of the Zionist criminals," according to the anonymous ILF representative who was interviewed in Jordan. The assertions of a terrorist connection were considered unreliable from the time they first appeared in the press.

Contrary to the this group’s declaration, all of the evidence indicates that the incident was an unfortunate and tragic accident. After an extensive investigation, it was determined that the explosion resulted from the ignition of flammable vapors that had accumulated in a storage tank during legitimate activity at the facility. Russ Elveston, of the Houston South Occupational Safety and Health Administration (OSHA) office, confirmed that the incident was not a terrorist act. [167] Elveston reaffirmed that there was nothing found to support or to suggest that that the Islamic Liberation Front had any role. In short, he indicated that a condition responsible for the magnitude of the explosion had developed over the course of a couple of weeks.

Although the claim of responsibility made by the Islamic Liberation Front had little impact on the local Channelview and greater Houston population, this case was included in the empirical analysis of chemical facility attacks largely to illustrate the effect that a terrorist group might have simply by claiming responsibility for an accident. A terrorist does not actually have to perpetrate an attack in order to achieve a psychological effect. The fact that this claim was made at a time, the early 1990s, when sensitivity about terrorist activities inside the U.S., both among the general population and law enforcement agencies, was far lower than it is today might account for the fact that it went relatively unnoticed. From the outset, moreover, there was little indication of intentional damage or sabotage at the site, which undercut terrorist suggestions of culpability.

[166] Jamal Halaby, “Extremists claim responsibility for U.S. chemical factory blast” *Associated Press*, 13 July 1990.
[167] Personal communication, 20 July 2004. OSHA Houston South Area Office, 17625 El Camino Real, Suite 400, Houston TX 77058, Phone: (281) 286-0583, <www.houston.feb.gov/osha.htm>.

Case 12

Location: Multiple Locations, Saudi Arabia

Date: Spring / Summer 2004

Perpetrator: Unknown

Target: ABB Lummas Global Inc. (Representative Target)

Tactic: Firearm Attacks

Motive: Anti-American; anti-West

Incident Description: Recent articles run by several news agencies have reported attacks against foreign nationals, including U.S. citizens, who are employed in Saudi Arabia, specifically in those industries involved in petroleum production and processing.[168,169,170] In light of these attacks, some of which have resulted in the deaths of Westerners, the security and safety of non-Arab employees in such locations is in serious doubt. The U.S. government has urged Americans to leave the Saudi kingdom insofar as the safety of U.S. workers was more important than any effect on oil supplies or the Saudi economy. The U.S. ambassador to Saudi Arabia issued a terse message saying "Go home. We cannot protect you."[171] One of the companies affected is the Houston-based ABB Lummus Global Inc., whose offices were attacked recently by four gunmen in an effort to encourage Saudi nationals to join the resistance against the U.S. occupation of Iraq.

Although these are not direct attacks against critical infrastructure, they are having an effect that is similar. Saudi oil production depends upon the specialized knowledge and know-how of foreign workers, without whom the maintenance of the Saudi oil industry infrastructure and the continuance of operations there could be jeopardized. This is especially true given that Saudi Arabia is being urged by the United States to increase its oil output to meet worldwide demands. Through a sustained campaign, the terrorists are weakening the oil industry infrastructure without destroying it, i.e., disruption without the destruction. They are impacting the oil infrastructure indirectly, which may interfere with the normal functioning of the U.S. economy if such attacks are escalated.

---

[168] "U.S. workers in Saudi Arabia advised to leave," *USA Today*, 3 May 2004, <www.usatoday.com>.
[169] "Americans leaving Saudi Arabia in droves," *World Net Daily, Geostrategy-Direct Intelligence Brief*, 17 June 2004, <www.worldnetdaily.com>.
[170] Pauline Jelinek, "U.S. urges Americans to exit Saudi Arabia," *Christian Broadcasting Network News*, 15 June 2004, <cbn.org/cbnnews/>.
[171] "U.S. workers in Saudi Arabia advised to leave," *USA Today*.

Section 4

THE DECIDe FRAMEWORK

A. DECIDe Framework Overview

This study was undertaken to develop a greater understanding of the factors and dynamics that induce terrorists to attack critical chemical infrastructure. Just as importantly, it was designed to "operationalize" the resulting research in a form that might enable analysts and policymakers to better mitigate future threats to chemical CI. The Determinants Effecting Critical Infrastructure Decisions (DECIDe) Framework – presented in detail in CNS' August 2004 study – was created as a tool to evaluate the likelihood that certain terrorist groups might attack various types of critical infrastructure.

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 4.1.) 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 identified in CNS' initial critical infrastructure study and expanded upon in this work.

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.

B. Critical Chemical Infrastructure Refinements

Findings relating to critical chemical infrastructure as identified in this study enable the DECIDe Framework to be refined to better suit the needs of analysts who desire to analyze the propensity of individual terrorist groups to specifically target chemical CI. Generally speaking, the modifications required to further focus the framework on a particular infrastructure type are minor. They principally involve those elements of the decision-making process that make attacks on critical chemical infrastructure more attractive or subjectively more feasible relative to other target types in the eyes of perpetrators. This section of the report summarizes those changes that should be made to best adapt the framework to the context of critical chemical infrastructure.

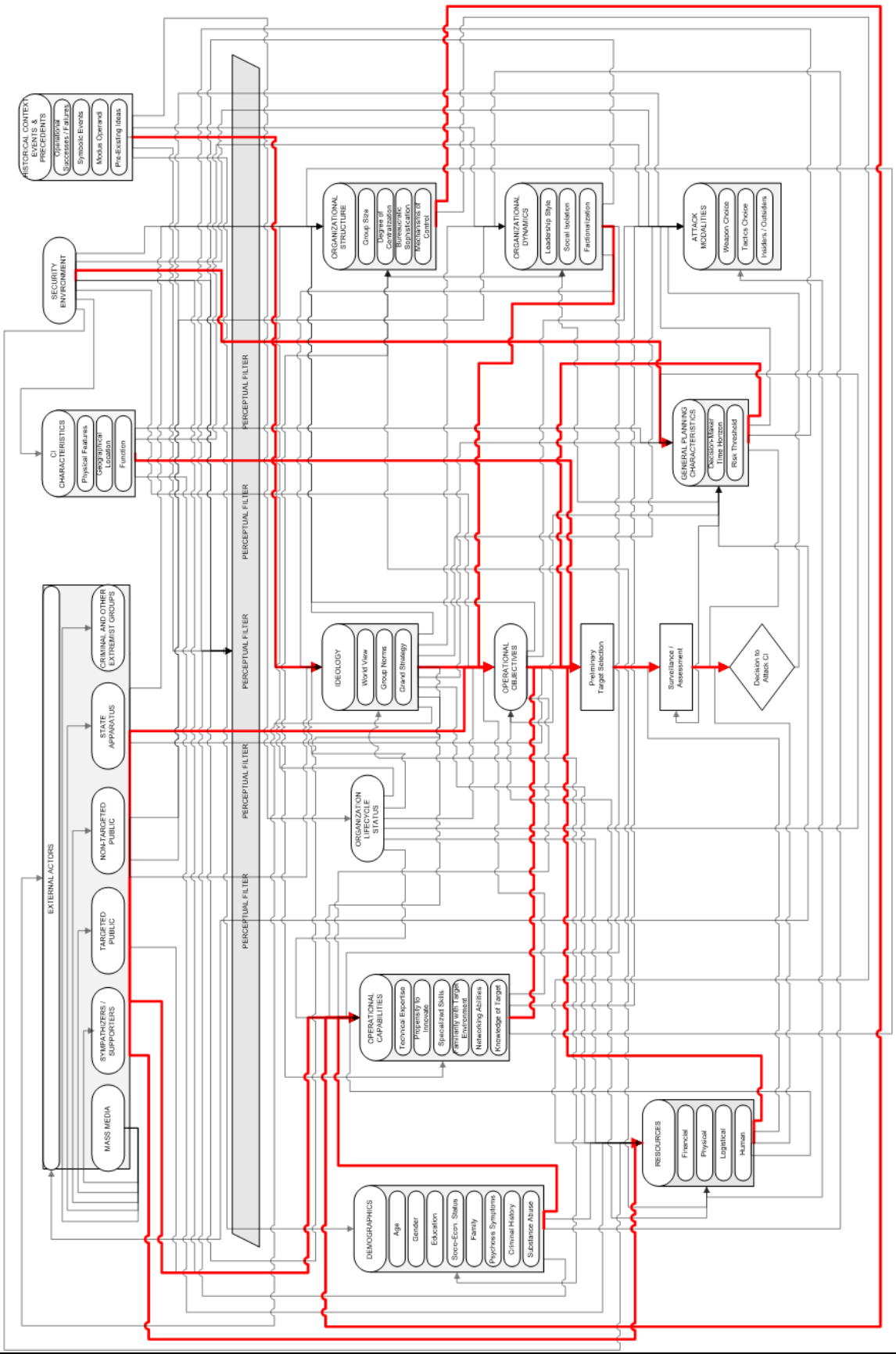


Figure 4.1: Contributing Factors Diagram

Regarding the framework modifications, two points should be emphasized. First, most factor influences have the same effect on target selection in the context of generic CI as in context of chemical-related infrastructure. Those elements of the framework that do not change will not be discussed. Second, perpetrators might follow one of two different "routes " in the process of deciding to target a critical chemical infrastructure target. In the first case, a terrorist group will have a propensity to attack critical infrastructure in general, and will settle on chemical-related infrastructure because the target is relatively more attractive (especially in terms of fulfilling operational objectives and in terms of being accessible to the terrorists relative to their capabilities. In the second case, a terrorist group may have a particular interest in engaging in CBRN terrorism and will settle on a critical chemical infrastructure target because it is the best way for the group to achieve an unconventional chemical attack. Analysts using the framework should be careful to consider the groups they are assessing in the context of one or the other of these paths.

The following pages present the particular modifications that should be made within each step of the framework design. Appendix V provides an abbreviated step-by-step walkthrough of the revised process.[172]

C. Step 1 Modifications

Step 1 is designed to serve as an initial investigation into a group's "known" desire to attack critical infrastructure. To specifically determine if a group is interested in attacking critical chemical infrastructure – rather than CI generally speaking – analysts should consider:

1) Is there evidence the group is planning to attack chemical-related infrastructure in the short to medium term?

2) Has the group attacked or made serious attempts to attack chemical-related infrastructure in the 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 chemical infrastructure and analysts can proceed to the next step in the framework.

D. Step 2 Modifications

Step 2 is designed to collect the data needed to use of the framework's subsequent factor analysis tools. In order better evaluate a group's particular interest in targeting chemical CI, Step 2 is modified to establish data requirements more directly related to critical chemical infrastructure. Specifically, it is recommended that analysts seek answers to the following questions:

1) Has the group expressed interest in conducting a CBRN attack or chemical attack, in particular?

2) What level of knowledge does the group have concerning various aspects of the chemical industry, in particular relating to processes and procedures?

3) What does the group perceive the functionality of chemical-related infrastructure to be and how do the view the consequences that might be expected from a successful attack against this type of infrastructure?

[172] For a full discussion of the framework, readers should refer to Chapter 5 of CNS' "Assessing Terrorist Motivations for Attacking Critical Infrastructure."

4) How has the media recently portrayed the importance and / or vulnerability of chemical-related infrastructure? Are group members likely to have seen these reports?

5) How does the group perceive security around chemical critical infrastructure targets relative to those around other types of infrastructure targets?

6) What level of publicity might the group expect if they successfully attack a chemical CI target?

E. Step 3 Modifications

Step 3 is designed to provide analytical processes that use known information about target selection factors to infer greater understanding about factors in which information is more ambiguous. The following changes have been made to the framework's factor analysis step to improve its ability to make assessments about terrorist interest in targeting critical chemical infrastructure.

Ideology: No changes to data requirements. Revised factor analysis diagram. (See page 96.)

Organizational Structure: No changes to data requirements. Revised factor analysis diagram. (See page 97.)

Demographics: No changes to data requirements. Revised factor analysis diagram. (See page 99.)

Operational Capabilities: Revised data requirements look for particular information concerning the group's levels of knowledge and skills relating to chemicals and industrial chemical processes. Revised factor analysis diagram. (See page 101.)

External relations: Revised data requirements look for particular information concerning coverage the media may have provided concerning the importance or vulnerability of critical chemical infrastructure. Revised factor analysis diagram. (See pages 102-103.)

Critical Infrastructure Characteristics: Revised data requirements seek information regarding: 1) how the group perceives the functionality of chemical-related infrastructure and what the consequences of a successful attack against such infrastructure might be; 2) how vulnerable the group perceives chemical CI to be relative to other potential targets; and 3) how much publicity the group expects to receive by attacking critical chemical infrastructure. (See page 104.)

F. Step 4 Modifications

Step 4 is designed to assist analysts in assessing a group's operational objectives and capabilities to determine whether a chemical CI attack is within their scope of interest and potential. These portions of the framework remain largely the same. While working through Step 4, however, it is recommended that analysts keep in mind the following facts:

1) If a terrorist group wants to attack chemical CI – and luck is taken out of the equation – some level of understanding of the industry and facility is required to conduct a successful luck.

2) If a group wants to cause large numbers of casualties by attacking a critical chemical infrastructure, they will need at least some knowledge of chemistry in order to know which chemicals are sufficiently toxic and how these chemicals might be expected to function when released.

3) If a group wants to release TICs, it must be able to both overcome physical security protecting the chemical facility as well as any automatic safeguards designed to prevent or mitigate unintentional releases. Terrorists must take into account the possibility that the impact of their attack could be curtailed by these systems.

4) As a variety of government studies and news exposés have demonstrated, chemical facilities around the nation continue to have fairly low levels of physical protection, especially when compared to other infrastructure such as airports, water treatment plants and nuclear power plants. This fact suggests that the capabilities required for attacking chemical CI are often relatively low, and that many groups – and even lone actors – possess the latent potential to do significant harm at such facilities under the right circumstances.

5) The Union Carbide tragedy in Bhopal, India may demonstrate how much damage a single individual can do in a large chemical facility. This highlights the importance – and danger – of "insiders" who might actively sabotage chemical CI. Although the empirical data does not show many cases of insider-based terrorist attacks against chemical facilities, this is a matter that requires significant attention.

Finally, in the last part of Step 4 – in which target selection is assessed – analysts should remember to make their final determination based on both: chemical critical infrastructure relative to other targets – including other types of critical infrastructure), as well as relative to other types of attacks using chemical agents. (It could be argued, for example, that attacking a chemical facility is easier than a group acquiring a chemical weapon, since they don't have to make, steal, ship, store etc. any dangerous chemicals.)

Section 5

Conclusion

Due to the paucity of data, particularly the reliance on only three cases in which terrorists have actually unequivocally targeted an industrial chemical production facility, any discussion of terrorist motives for attacking critical chemical infrastructure must be somewhat speculative. Nonetheless, observations based on the historical record may provide insight into potential future terrorist motivations for attacking such targets.

The first point to note is that – of the actual attacks attributable to terrorist activity identified in CrITIC – all were carried out in-country by domestic groups. The terrorists considered the land on which the facility was located to be part of their territory or "homeland." The primary motivation of all three of the groups that attacked chemical production plants – facilities that clearly fall into the critical infrastructure category – was their opposition to the ruling government. Of the attacks on non-production facilities, the motivations for two-thirds (four of six) of the cases were also linked to internal politics.

The "Peace Conquerors" group (cases #6 and #7) appears to have been a transnational endeavor, or it was an individual or small group making spurious international claims. None of the genuine incidents can be interpreted as a terrorist group targeting chemical infrastructure on foreign soil, as would be the case if al-Qa`ida targeted a domestic U.S. facility. If one extrapolates narrowly, which may well be misleading, the historical record suggests that the most likely scenario for a terrorist attack on a domestic U.S. chemical facility would be carried out by domestic U.S. terrorists. As discussed in Section 2, however, recent information related to al Qa`ida indicates that this "trend" may be changing.

Intense disagreement with U.S. policies has also been obvious in all three cases of attacks on actual production facilities. The proclaimed motivations were not so much to harm the U.S. directly, but rather to symbolically protest U.S. foreign policies that affected the perpetrator's own homelands (cases #2 and #3) or another country (case #1). Three cases appear in the empirical record in which targeting may have occurred due to a facility's perceived link to the U.S. military (cases #1, #7 and #11). While not directly impacting domestic U.S. critical infrastructure, this trend should be of concern to American and British chemical companies operating facilities abroad. The choice of two of the three production facility attacks appears to have been motivated to some extent by alleged U.S. military relations with a foreign country (case #1) or by the U.S. military presence in their homeland (case #2).

The targeting of petroleum production, transfer, and storage facilities has not been exhaustively considered in this analysis, as this would more accurately represent an attack on the energy infrastructure rather than on industrial chemical facilities. While petroleum and petroleum by-products are the feed stocks for modern chemical compounds,[173] oil pipelines and refineries are not generally considered chemical infrastructure. With increased agitation in the Middle East and the perception by many Muslims that the U.S. invasion of Iraq in 2003 was motivated by a desire to control oil production, the petrochemical industry may well become the target of increased terrorist attacks. Case #12 may be indicative of an increased blurring of the differences between the oil and chemical industries. Although thwarted before it could be actualized, the Wise County incident (Operation Sourgas, Section 2), demonstrates how both ideology and practical considerations can dovetail in domestic terrorist targeting of chemical facilities.

---

[173] For every ton of crude oil, six percent is diverted to ethylene, propylene and benzene production. Less than one percent is used for the synthesis of fine chemicals, which are subsequently converted to pharmaceutical, personal care and other consumer products. For more on the relationship between petroleum and the chemical industry, see: Mark M. Green and Harold A. Wittcoff, *Organic Chemistry Principles and Industrial Practices*, Wiley-VCH, 2003.

Very little can be deduced from the cases concerning capabilities required by terrorists to attack. To do significant damage that truly impacts the U.S. critical infrastructure – rather than inflicting symbolic damage or causing large numbers of casualties – would require the large-scale targeting of select facilities, especially those that are key manufacturers of critical chemicals or single producers of raw chemicals. Most potentially catastrophic for the U.S. chemical critical infrastructure would be a coordinated attack on a number of facilities responsible for key precursors, the disruption of which would cause a bottleneck blockage. Fortunately, the selection of such facilities would require sophisticated knowledge of chemical manufacturers, industrial processes, distribution, and warehousing. It would also require a substantial effort by a relatively large, well-financed terrorist group with access to individuals with specific scientific or technical knowledge. That said, the Bhopal and Channelview, Texas cases – which may simply have been accidents – demonstrate that damage at even solitary plants can yield significant human and economic consequences. Both incidents also suggest that high levels of technical expertise are not required to cause major accidents. However, as was considered in Section 2, even sophisticated attacks, such as those conducted by Serb forces against the Petrokemija facility, may not succeed in obtaining a perpetrator's desired operational objectives.

Data on the causes of industrial incidents over a thirty-year period indicate that only 1% were attributable to sabotage or arson.[174] The leading cause of accidents, 44%, was found to be mechanical failure. Although it may be that unsolved incidents were the result of terrorist activity, no such case was detected in our search of the empirical record.[175] The historical record, while extremely limited, reveals that the overwhelming majority of terrorist attacks on industrial chemical facilities involved the use of bombs or other incendiary devices as opposed to sabotage. Furthermore, all of the terrorist methods carried out to date reflect crude methods of causing damage to the chemical infrastructure. This suggests, if the historical record is indicative of future terrorist attacks, that the number one priority should be increasing basic perimeter security in order to prevent a bomb or other incendiary device from harming a facility. The structural integrity of storage tanks and other vessels containing large volumes of flammable materials should be reinforced wherever possible.

The 1990 Channelview ARCO accident (case 11) may represent the most likely scenario in the future, and one that can be readily managed. The southeastern area of Texas has been the site of some of the worst industrial chemical accidents in U.S. history.[176,177] The ARCO accident occurred less than a year after an explosion and fire at a plastics production facility owned by Phillips Petroleum Company, in which twenty-three people were killed and 132 injured. Three years earlier, in October 1987, more than four thousand residents were evacuated from the Texas City area in the wake of an accidental release of highly corrosive hydrofluoric acid from a Marathon Petroleum Company facility. More than 225 people suffered acid-related injuries, but there were no fatalities. The worst industrial accident in U.S. history occurred in Texas City on 16 April 1947, when a ship transporting ammonia nitrate fertilizer exploded at the dock. The next day, another ship full of fertilizer blew up. It is estimated that the two incidents resulted in at least 576 fatalities and over 5000 injuries. Monetary losses in 1947 were estimated at $47 million.

Another aspect to consider is that terrorists will try to exploit a well-publicized accident by claiming responsibility. The Bhopal and Channelview incidents (cases #10 and #11, respectively) point to the vital need to establish causation when something does go wrong at an industrial facility, and to establish it as quickly and unambiguously as possible. Investigations need to be open and involve members of the local communities that were or possibly would have been directly affected by an incident. Trusted spokesmen need to be identified and better relationships established with local communities. This may be a local fire chief, a familiar news reporter or another civic leader who is readily recognized by the greater populace.

---

[174] Marsh & McLennon, "Large Property Damage Losses in the Hydrocarbon-Chemical Industries a thirty-year Review," 18th Edition, Marsh and McLennan Protection Consultants, New York, 1998.
[175] Note: such accidents have not been specifically reviewed, so the relative quantity is unknown.
[176] Rad Sallee, "Houston area no stranger to industrial disasters," *The Houston Chronicle*, 24 December 1996.
[177] Trevor A. Kletz, *What Went Wrong? Case Studies of Process Plant Disasters*, Gulf Professional Publishing, 1998.

A novel form of terrorist attack might involve a pseudo-"copycat" incident following a genuine industrial accident. A terrorist group, after observing the fear, panic, and destruction associated with an accident, might be inspired to exploit those effects for malicious purposes. This would be highly effective in impacting a population agitated by a recent industrial accident. It would also immediately engender challenges to the veracity of initial reports that an incident was accidental rather than an unattributed case of terrorism.

While the small number of terrorist-initiated attacks on chemical facilities is heartening, this situation makes discerning motivational patterns and formulating conclusions problematic. Overall the historical record suggests that the targeting of chemical infrastructure has until now been motivated primarily by domestic political conflicts. Opposition to U.S. foreign policy has also been a motive in attacks on American and German-owned chemical facilities overseas. These may well be viewed as "softer," more attractive targets compared to plants inside the U.S.

Before taking too much consolation in the fact that few empirical cases of critical chemical infrastructure attacks exist, the following U.S. Department of Justice comments should be kept in mind:

> "There has yet to be a toxic chemical release from a facility in the U.S. as a result of terrorist or criminal activity. The predictive value of this fact is limited, however. First, in contrast to the lack of terrorist incidents aimed at industrial chemical releases during the entire history of the United States, in the last two years alone law enforcement thwarted two attempts to cause such a chemical release. These recent events suggest that there may be a change in trends relating to such crimes and that the past may not be the most reliable barometer of future events in regard to criminal and terrorist efforts to cause mass damage and casualties through means that may include toxic industrial chemical releases."[178]

Such a warning is particularly wise in light of the changing nature of terrorism during the last decade. The 1993 New York City World Trade Center bombing, the 1995 Tokyo subway sarin attack and Oklahoma City bombing, the 1998 U.S. embassy bombings in Kenya and Tanzania, and September 11, 2001 suggest a disturbing trend in terrorism toward attacks involving unconventional tactics, mass casualties and mass damage. To adequately address this possible shift, analysts and decision-makers should remain mindful of the wide range of rational, functionally-driven motivations that terrorists can have for attacking critical chemical infrastructure. In particular they should consider the possibility that such infrastructure might especially be targeted to: cause human casualties; cause physical destruction; cause environmental contamination; damage the economy; disrupt strategic industrial functions; provide supplies of chemicals (for later use as weapons); influence the general public; enhance terrorist leverage in negotiations; and facilitate terrorist organization building efforts.

[178] Department of Justice, 2000, p. 28.

BIBLIOGRAPHY

The Agency for Toxic Substances and Disease Registry's (ATSDR) 1999 report, "Industrial Chemicals and Terrorism: Human Health Threat Analysis, Mitigation and Prevention," Department of Health and Human Services, 1999. Available at http://www.mapcruzin.com/scruztri/docs/cep1118992.htm, accessed September 20, 2004.

American Chemical Council website, available at http://www.americanchemistry.com.

"Americans Leaving Saudi Arabia in Droves," *WorldNetDaily, Geostrategy-Direct Intelligence Brief*, June 17, 2004. Available at www.worldnetdaily.com, accessed September 20, 2004.

"ARCO Petrochemical Unit Blast Jolts Markets," *Oil & Gas Journal*, July 1990, p. 28.

Peter Avis, "Planned Chemical Plant Stirs Hopes and old Fears in India," *The Toronto Star*, February 4, 1995.

Justin Bachman and Laura Vozzella, "FBI Says Bomb Plot Thwarted; Gas Blast Could Have Wiped Out 'Half of Wise County'," *Fort Worth Star-Telegram*, April 24, 1997.

Scott Baldauf, "Bhopal Gas Tragedy Lives on, 20 Years Later," *The Christian Science Monitor*, May 4, 2004.

"Bayer's Plant Resumes After Terrorist Attack," *Chemical Week*, June 29, 1983, p. 14.

James C. Belke, "Chemical accident risks in U.S. industry – A preliminary analysis of the accident risk data from U.S. hazardous chemical facilities," U.S. Environmental Protection Agency, September 25, 2000.

"Bhopal Methyl Isocyanate Investigation Team Report," Union Carbide Corporation, Danbury, Connecticut, March 1985.

Christine Biederman, "Ku Klux Klowns," *Texas Monthly*, January 1998.

"Blast at Union Carbide," *The Courier-Mail* (Brisbane, Australia), July 6, 1983.

"Bomb damages Bayer building," Associated Press, June 22, 1985.

Chris Brice, "Terrorism has Become the New Boom Industry," *Courier-Mail (*Brisbane, Australia*)*, June 28, 1985.

Jackson B. Browning, "Union Carbide: Disaster at Bhopal," 1993. Originally appeared in Jack A. Gottschalk, ed., *Crisis Response: Inside Stories on Managing Under Siege*, (Detroit, MI:Visible Ink Press). Available at www.bhopal.com/pdfs/browning.pdf, accessed September 20, 2004.

Rob Buschmann, "Risk Assessment in the Presidents National Strategy for Homeland Security," Congressional Research Service, October 31, 2002.

"The Business of Chemistry: Essential to Our Quality of Life and the New Economy," American Chemical Council Fact Sheet, July 31, 2002. Available at www.accnewsmedia.com/docs/300/241.pdf, accessed September 20, 2004.

"Calendar of Conspiracy, Volume 1, Number 4: A Chronology of Anti-Government Extremist Criminal Activity, October to December 1997," Anti-Defamation League, February 18, 1998.

Ricardo Cappelli and Nicola Labanca, "Proliferation and Disarmament of Chemical Weapons in the NATO Framework: Lessons from History," University of Sienna, 2000.

The Center for Nonproliferation Studies "Assessing Terrorist Motivations for Attacking Critical Infrastructure," Prepared for Lawrence Livermore National Laboratory, August 2004.

"Chemical and Biological Medical Treatment Symposium: Croatia, Applied Science and Analysis Newsletter, October 1998. Available at http://www.asanltr.com/ASANews-98/cbmts-indi.html, accessed September 20, 2004.

"Chemical Plant Security," Congressional Research Service, January 20, 2004.

"Chemical Warfare Conventions Changed Over Fertilizer Plant Attacks," Washington Times International Reports.net, December 1998. Available at http://www.internationalspecialreports.com/europe/01/croatia/chemicalwarfare.html, accessed September 20, 2004.

"Cologne Bombing," *Financial Times*, October 1, 1986.

Barbara Crossette, "Bhopal's Tragedy Revisited; 10 Years After the Gas," *New York Times*, December 11, 1994.

C.J.M. Drake, *Terrorists' Target Selection* (New York: St. Martin's Press, Inc, 1998), p. 80.

William Drozdiak, "Bombs hit West German Targets: Leftists say Attacks Linked to Summit," *Washington Post*, April 30, 1985.

"Dynamite Attacks Plunge Lima into Darkness," United Press International, May 27, 1983.

"Econuts Bomb Two Jets," *Telegraph* (Sydney, Australia), June 24, 1985.

Lois Ember, "Worst-Case Scenario for Chemical Plant Attack," Chemical & Engineering News, 80 (March 2002), p. 8.

Steven Erlanger, "Bombing Unites Serb Army As It Debilitates Economy – Production Cut in Half, Experts Say," *New York Times*, April 30, 1999.

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.

Joseph B. Fleming, "Terrorist Bombs Planted at West German Offices," United Press International, May 3, 1985.

V.P. Gagnon Jr., *The Myth of Ethnic War: Serbia and Croatia in the 1990s* (Ithaca: Cornell University Press, 2004).

Mark M. Green and Harold A. Wittcoff, *Organic Chemistry Principles and Industrial Practices,* Wiley-VCH, 2003.

Jamal Halaby, "Extremists Claim Responsibility for U.S. Chemical Factory Blast," Associated Press, July 13, 1990.

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. Available at http://www.ciaonet.org/wps/hob03/, accessed September 20, 2004.

Information Bank Abstracts, *New York Times,* February 24, 1974, p. 7.

Faezah Ismail, "Our Responsibility to the Future," *New Straits Times* (Malaysia), January 24, 1995.

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

Pauline Jelinek, "U.S. Urges Americans to Exit Saudi Arabia," Christian Broadcasting Network News, June 15, 2004. Available at www.cbn.org/cbnnews/, accessed September 20, 2004.

Jeff Johnson, "Chemical Accident Data: Plethora of Confusion," *Chemical & Engineering News,* 77 (March 1999), p. 22-23.

Ashok S. Kalelkar, "Investigation of Large-Magnitude Incidents: Bhopal as a Case Study," presented at the Institution of Chemical Engineers Conference on Preventing Major Chemical Accidents, London, England, May 1998. Available at www.bhopal.com/pdfs/casestdy.pdf, accessed September 20, 2004.

Peter Kammerer, "Dead Men Walking at Work Every Day," *South China Morning Post*, May 2, 2004.

Theodore Karasik, *Toxic Warfare*, RAND 2002.

Trevor A. Kletz, *What Went Wrong? Case Studies of Process Plant Disasters,* Gulf Professional Publishing, 1998.

Dominique LaPierre and Javier Moro, *Five Past Midnight: The Epic Story of the World's Deadliest Industrial Accident* (New York: Warner Books, 2002).

Debora MacKenzie, "Fresh Evidence on Bhopal Disaster: Documents Suggest U.S. Company was Responsible for Plant's Design and cut Investment to Maintain Control," *New Scientist,* December 7, 2002. Available at www.NewScientist.com, accessed September 20, 2004.

David Maraniss, "Texas Chemical Plant Blast Kills 17," *Washington Post*, July 7, 1990.

Aileen McCabe, "Balkans: Bombs Rain as Leaders Meet to Discuss Peace," *Ottowa Citizen*, September 8, 1995.

Marsh & McLennon, "Large Property Damage Losses in the Hydrocarbon-Chemical Industries: a Thirty-year Review," 18th Edition, Marsh and McLennan Protection Consultants, New York, 1998.

Boris Mesaric, Chairman of the Board, Petrochemica, telephone interview with CNS Research Associate, September 13, 2004.

"Methyl Isocyanate: How it is Made," *Chemical Week*, December 19, 1984.

Michael R. Meyer and Michael Smith, "Peru: The 'Shining Path' to Terror," *Newsweek*, June 13, 1983.

Edward F. Mickolus, *Transnational Terrorism: A Chronology of Events, 1968-1979* (Westport, CT: Greenwood Press, 1980).

Edward F. Mickolus, Todd Sandler, Jean M. Murdock, *International Terrorism in the 1980's: A Chronology of Events*, Vol. 1, 1980-1983 (Ames: Iowa State University Press, 1989).

John Motef et al., "Critical Infrastructures: What Makes an Infrastructure Critical?" Congressional Research Service, January 29, 2003.

"New Bomb Threats by 'Peace' Group," *Telegraph* (Sydney, Australia), June 26, 1985.

S. O'Conner, "No Threat Before Factory Bombing," *Telegraph* (Sydney, Australia), July 5, 1985.

Personal communication, July 20, 2004. OSHA Houston South Area Office, Houston TX

"Phillips to Pay $4 Million for Fatal Safety Violations: 23 Workers Died in Chemical Plant Blast," *Atlanta Journal and Constitution*, August 23, 1991.

Eric Pianin, "Study Assesses Risk of Attack on Chemical Plant," *Washington Post*, March 12, 2002.

"Police Detain 500 in Peru Bombings," *New York Times*, May 30, 1983.

"Police Say They are Taking Seriously Claim by 'Peace Conquerors'," Associated Press, June 24, 1985.

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).

Marc S. Reisch, "Twenty Years After Bhopal," *Chemical & Engineering News*, 82 (23), 7 June 2004.

Nancy A Renfroe and Joseph L. Smith, "*Threat/Vulnerability Assessments and Risk Analysis. Whole Building Design Guide*," 2004. Available at http://www.wbdg.org/design/res-print.php?rp=27, accessed September 20, 2004.

Simon Reyonolds, "The Price of Tragedy Rises - Industrial Risk Rates are out of Step with the New Size of Losses," *Financial Times*, September 9, 1991.

Charles A Russell and Robert E Hildner, "The Urban Guerrilla in Latin America," *Air University Review* (September-October 1973). Available at http://www.airpower.maxwell.af.mil/airchronicles/aureview/1973/sep-oct/russell.html, accessed September 20, 2004.

S.157 "The Chemical Security Act of 2003." Available at http://www.theorator.com/bills108/s157.html, accessed September 20, 2004.

"Sabotage? U.S. Dismisses ARCO Explosion Claim," *St. Louis Post-Dispatch* (Missouri), July 14, 1990.

Rad Sallee, "Houston Area no Stranger to Industrial Disasters," *Houston Chronicle,* December 24, 1996.

Linda-Jo Schierow, "Chemical Plant Security," Congressional Research Service, January 20, 2004.

Bruce Schneier, *Secrets and Lies: Digital Security in the Networked World* (Wiley Publishing, Inc., 2004).

Jim Schutze, "Four Accused of Plot to Blow Up Gas Plant; Armored Car Robbery Part of Plan," *Houston Chronicle*, April 24, 1997.

Jim Schutze and Richard Stewart, "Texas Bomb Plot Suspects Klan Officers, Group Says," *Houston Chronicle,* April 25, 1997.

John Stephenson, "Federal Action Needed to Address Security Challenges at Chemical Facilities," General Accounting Office, February 23, 2004.

Frank Swoboda, "Settlement set in '90 Plant Blast," *Washington Post*, January 4, 1991.

"Sydney Plants Threatened," *New York Times*, December 9, 1984.

"Terror Group in Australia?" *Telegraph* (Sydney, Australia), July 9, 1985.

Mazhar Ullah, "Court Refuses to Reduce Murder Charge Against Bhopal Chief," *Guardian* (London), August 29, 2002. Available at www.guardian.co.uk, accessed September 20, 2004.

U.S. Chemical Safety and Hazard Investigation Board, "Hazard Investigation: Improving Reactive Hazard Management," Report No. 2001-01-H, October 2002.

U.S. Census Bureau, "2002 NAICS Codes and Titles." Available at http://www.census.gov/epcd/naics02/def/NDEF325.HTM#N325, accessed September 20, 2004.

U.S. Department of Homeland Security "Characteristics and Common Vulnerabilities Report for Chemical Facilities," Version 1 (rev.1), July 17, 2003.

"U.S. 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.

"U.S. Workers in Saudi Arabia Advised to Leave," *USA Today*, May 3, 2004.

Laura Vozzella, "Sentences For Four Would-Be Bombers Too Tough Court Says," *Fort Worth Star-Telegram*, June 24, 1999.

Penny Wark, "The Toxic Legacy of the Explosion of a Pesticide Factory in Bhopal is Still Felt 20 Years on," *Times* (London), May 25, 2004.

"Weapons of Mass Destruction, Toxic Industrial Materials, and the Use of Obscuration," in *Combined Arms Operations in Urban Terrain, Department of the Army Field Manual*, No. 3-06.11. Appendix F, February 28, 2002.

"West German Bomb Attack Foiled," *Washington Post*, December 12, 1989.

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

"Why the People's War in Peru is Justified and Why it is the Road to Liberation," text of speech by Heriberto Ocasio (National Spokesman, Committee to Support the Revolution in Peru, Berkeley CA), May 1995.

Andrew Wood and Shelina Shariff, "Fallout from Channelview Explosion Keeps on Coming," *Chemical Week*, June 24, 1990.

Ian Young and Shelina Shariff, "MTBE Still Leading the way in Global Octane Surge," *Chemical Week*, July 18, 1990.

Appendix I

KEY TERMS and DEFINITIONS from "ASSESSING TERRORIST MOTIVATIONS TO ATTACK CRITICAL INFRASTRCTURE"*

The following terms were identified and discussed in CNS' report "Assessing Terrorist Motivations to Attack Critical Infrastructure." They are used in the DECIDe Framework to evaluate terrorist motivations for attacking critical infrastructure. While these factors are not the only important dynamics that affect terrorist decision-making, they are those that CNS' research has determined to be most influential in determining target selection. The terms are presented in alphabetical order.

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.

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?).

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?).

* The original discussion of the terms presented in this Appendix may be found in Chapter 2 (pages 18 to 24) of CNS' report, "Assessing Terrorist Motivations to Attack Critical Infrastructure."

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.

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?

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.

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.

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.

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,[179] 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.

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

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

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.

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.

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.

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.

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.

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.

Appendix II

EXECUTIVE SUMMARY from "ASSESSING TERRORIST MOTIVATIONS TO ATTACK CRITICAL INFRASTRCTURE"*

"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[180]

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 on 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 original Executive Summary can be found on pages vi to xvii of CNS' report, "Assessing Terrorist Motivations to Attack Critical Infrastructure."

[180] The White House, "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. 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.

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.

Appendix III

THE CHEMICAL INDUSTRY AS DEFINED BY THE NORTH AMERICAN INDUSTRY CLASSIFICATION SYSTEM*

NAISC Code	Chemical Industry Activity	Description
325110	Petrokemijal Manufacturing	This industry comprises establishments primarily engaged in (1) manufacturing acyclic (i.e., aliphatic) hydrocarbons such as ethylene, propylene, and butylene made from refined petroleum or liquid hydrocarbon and/or (2) manufacturing cyclic aromatic hydrocarbons such as benzene, toluene, styrene, xylene, ethyl benzene, and cumene made from refined petroleum or liquid hydrocarbons.
325120	Industrial Gas Manufacturing	This industry comprises establishments primarily engaged in manufacturing industrial organic and inorganic gases in compressed, liquid, and solid forms.
325131	Inorganic Pigments	This industry comprises establishments primarily engaged in manufacturing synthetic inorganic dyes and pigments, such as lakes and toners (except electrostatic and photographic).
325132	Organic Dyes and Pigments	This U.S. industry comprises establishments primarily engaged in manufacturing synthetic organic dyes and pigments, such as lakes and toners (except electrostatic and photographic).
325181	Alkalies and Chlorine	This U.S. industry comprises establishments primarily engaged in manufacturing chlorine, sodium hydroxide (i.e., caustic soda), and other alkalies often using an electrolysis process.
325182	Carbon Black	This U.S. industry comprises establishments primarily engaged in manufacturing carbon black, bone black, and lamp black.
325188	All Other Basic Inorganic Chemicals	This U.S. industry comprises establishments primarily engaged in manufacturing basic inorganic chemicals (except industrial gases, inorganic dyes and pigments, alkalies and chlorine, and carbon black).
325191	Gum and Wood Chemicals	This U.S. industry comprises establishments primarily engaged in (1) distilling wood or gum into products, such as tall oil and wood distillates, and (2) manufacturing wood or gum chemicals, such as naval stores, natural tanning materials, charcoal briquettes, and charcoal (except activated).

* All information in Appendix III is taken from the U.S. Census Bureau, "2002 NAICS Codes and Titles," <http://www.census.gov/epcd/naics02/def/NDEF325.HTM#N325>.

325192	Cyclic Crudes and Intermediates	This U.S. industry comprises establishments primarily engaged in (1) distilling coal tars and/or (2) manufacturing cyclic crudes or, cyclic intermediates (i.e., hydrocarbons, except aromatic Petrokemijals) from refined petroleum or natural gas.
325193	Ethyl Alcohol	This U.S. industry comprises establishments primarily engaged in manufacturing nonpotable ethyl alcohol.
325199	All Other Basic Organic Chemicals	This U.S. industry comprises establishments primarily engaged in manufacturing basic organic chemical products (except aromatic Petrokemijals, industrial gases, synthetic organic dyes and pigments, gum and wood chemicals, cyclic crudes and intermediates, and ethyl alcohol).
325211	Plastics Material and Resins	This U.S. industry comprises establishments primarily engaged in (1) manufacturing resins, plastics materials, and nonvulcanizable thermoplastic elastomers and mixing and blending resins on a custom basis and/or (2) manufacturing noncustomized synthetic resins.
325212	Synthetic Rubber (Vulcanizable Elastomers)	This U.S. industry consists of establishments primarily engaged in manufacturing synthetic rubber.
325221	Manufactured Cellulosic Fibers	This U.S. industry comprises establishments primarily engaged in (1) manufacturing cellulosic (i.e., rayon and acetate) fibers and filaments in the form of monofilament, filament yarn, staple, or tow or (2) manufacturing and texturizing cellulosic fibers and filaments.
325222	Manufactured Noncellulosic Fibers	This U.S. industry consists of establishments primarily engaged in (1) manufacturing noncellulosic (i.e., nylon, polyolefin, and polyester) fibers and filaments in the form of monofilament, filament yarn, staple, or tow, or (2) manufacturing and texturizing noncellulosic fibers and filaments.
325311	Nitrogenous Fertilizers	This U.S. industry comprises establishments primarily engaged in one or more of the following: (1) manufacturing nitrogenous fertilizer materials and mixing ingredients into fertilizers; (2) manufacturing fertilizers from sewage or animal waste; and (3) manufacturing nitrogenous materials and mixing them into fertilizers.
325312	Phosphatic Fertilizers	This U.S. industry comprises establishments primarily engaged in (1) manufacturing phosphatic fertilizer materials or (2) manufacturing phosphatic materials and mixing them into fertilizers.
325314	Fertilizers, Mixing Only	This U.S. industry comprises establishments primarily engaged in mixing ingredients made elsewhere into fertilizers.
325320	Pesticides and Other Agricultural Chemicals	This industry comprises establishments primarily engaged in the formulation and preparation of agricultural and household pest control chemicals (except fertilizers).

325411	Medicinals and Botanicals	This U.S. industry comprises establishments primarily engaged in (1) manufacturing uncompounded medicinal chemicals and their derivatives (i.e., generally for use by pharmaceutical preparation manufacturers) and/or (2) grading, grinding, and milling uncompounded botanicals.
325412	Pharmaceutical Preparations	This U.S. industry comprises establishments primarily engaged in manufacturing in-vivo diagnostic substances and pharmaceutical preparations (except biological) intended for internal and external consumption in dose forms, such as ampoules, tablets, capsules, vials, ointments, powders, solutions, and suspensions.
325413	Diagnostic Substances, In Vitro	This U.S. industry comprises establishments primarily engaged in manufacturing in-vitro (i.e., not taken internally) diagnostic substances, such as chemical, biological, or radioactive substances. The substances are used for diagnostic tests that are performed in test tubes, petri dishes, machines, and other diagnostic test-type devices.
325414	Biological Products, Except Diagnostics	This U.S. industry comprises establishments primarily engaged in manufacturing vaccines, toxoids, blood fractions, and culture media of plant or animal origin (except diagnostic).
325510	Paints and Coatings	This industry comprises establishments primarily engaged in (1) mixing pigments, solvents, and binders into paints and other coatings, such as stains, varnishes, lacquers, enamels, shellacs, and water repellant coatings for concrete and masonry, and/or (2) manufacturing allied paint products, such as putties, paint and varnish removers, paint brush cleaners, and frit.
325520	Adhesives and Sealants	This industry comprises establishments primarily engaged in manufacturing adhesives, glues, and caulking compounds.
325611	Soaps and Detergents	This U.S. industry comprises establishments primarily engaged in manufacturing and packaging soaps and other detergents, such as laundry detergents; dishwashing detergents; toothpaste gels, and tooth powders; and natural glycerin.
325612	Polishes and Sanitation Goods	This U.S. industry comprises establishments primarily engaged in manufacturing and packaging polishes and specialty cleaning preparations.
325613	Surfacants, Finishing Agents and Assistants	This U.S. industry comprises establishments primarily engaged in (1) manufacturing bulk surface active agents for use as wetting agents, emulsifiers, and penetrants, and/or (2) manufacturing textiles and leather finishing agents used to reduce tension or speed the drying process.

325620	Toilet Preparations	This industry comprises establishments primarily engaged in preparing, blending, compounding, and packaging toilet preparations, such as perfumes, shaving preparations, hair preparations, face creams, lotions (including sunscreens), and other cosmetic preparations.
325910	Printing Ink	This industry comprises establishments primarily engaged in manufacturing printing and inkjet inks and inkjet cartridges.
325920	Explosives	This industry comprises establishments primarily engaged in manufacturing explosives.
325991	Custom Compounding of Purchased Resin	This industry comprises establishments primarily engaged in (1) custom mixing and blending plastics resins made elsewhere or (2) reformulating plastics resins from recycled plastics products.
325992	Photographic Film, Paper, Plate and Chemical Products	This U.S. industry comprises establishments primarily engaged in manufacturing sensitized film, sensitized paper, sensitized cloth, sensitized plates, toners (i.e., for photocopiers, laser printers, and similar electrostatic printing devices), toner cartridges, and photographic chemicals.
325998	All Other Miscellaneous Chemical Products	This U.S. industry comprises establishments primarily engaged in manufacturing chemical products (except basic chemicals, resins, synthetic rubber; cellulosic and noncellulosic fiber and filaments; pesticides, fertilizers, and other agricultural chemicals; pharmaceuticals and medicines; paints, coatings and adhesives; soap, cleaning compounds, and toilet preparations; printing inks; explosives; custom compounding of purchased resins; and photographic films, papers, plates, and chemicals).

Appendix IV

THE TOP 20 INDUSTRIES REPORTING CHEMICAL PROCESSES THAT REQUIRE RMPs*

NAICS Code	Industry Type	Industry Description	Number of Reported Processes
42291	Farm Supplies Wholesalers	This industry comprises establishments primarily engaged in wholesaling farm supplies, such as animal feeds, fertilizers, agricultural chemicals, pesticides, plant seeds, and plant bulbs.	4,409
22131	Water Supply and Irrigation	This industry comprises establishments primarily engaged in operating water treatment plants and/or operating water supply systems. The water supply system may include pumping stations, aqueducts, and/or distribution mains. The water may be used for drinking, irrigation, or other uses.	2,059
22132	Sewage Treatment	This industry comprises establishments primarily engaged in operating sewer systems or sewage treatment facilities that collect, treat, and dispose of waste.	1,646
32411	Petroleum Refineries	This industry comprises establishments primarily engaged in refining crude petroleum into refined petroleum. Petroleum refining involves one or more of the following activities: (1) fractionation; (2) straight distillation of crude oil; and (3) cracking.	1,609
325199	All Other Basic Organic Chemical Manufacturing	This U.S. industry comprises establishments primarily engaged in manufacturing basic organic chemical products (except aromatic Petrokemijals, industrial gases, synthetic organic dyes and pigments, gum and wood chemicals, cyclic crudes and intermediates, and ethyl alcohol).	655
42269	Other Chemical and Allied Products Wholesalers	This industry comprises establishments primarily engaged in wholesaling chemicals and allied products (except agricultural and medicinal chemicals, paints and varnishes, fireworks, and plastics materials and basic forms and shapes).	607
49312	Refrigerated Warehousing and Storage Facilities	This industry comprises establishments primarily engaged in operating refrigerated warehousing and storage facilities. Establishments primarily engaged in the storage of furs for the trade are included in this industry. The services provided by these establishments include blast freezing, tempering, and modified atmosphere storage services.	549

* Shaded rows denote chemical manufacturing-related activities. All information in Appendix IV is taken from the U.S. Census Bureau, "2002 NAICS Codes and Titles," <http://www.census.gov/epcd/naics02/def/NDEF325.HTM#N325>.

211112	Natural Gas Liquid Extraction	This U.S. industry comprises establishments primarily engaged in the recovery of liquid hydrocarbons from oil and gas field gases. Establishments primarily engaged in sulfur recovery from natural gas are included in this industry.	533
325211	Plastics Material and Resin Manufacturing	This U.S. industry comprises establishments primarily engaged in (1) manufacturing resins, plastics materials, and nonvulcanizable thermoplastic elastomers and mixing and blending resins on a custom basis and/or (2) manufacturing noncustomized synthetic resins.	418
325188	All Other Basic Inorganic Chemical Manufacturing	This U.S. industry comprises establishments primarily engaged in manufacturing basic inorganic chemicals (except industrial gases, inorganic dyes and pigments, alkalies and chlorine, and carbon black).	358
49313	Farm Product Warehousing	This industry comprises establishments primarily engaged in operating bulk farm product warehousing and storage facilities (except refrigerated). Grain elevators primarily engaged in storage are included in this industry.	345
32511	Petrokemijal Manufacturing	This industry comprises establishments primarily engaged in (1) manufacturing acyclic (i.e., aliphatic) hydrocarbons such as ethylene, propylene, and butylene made from refined petroleum or liquid hydrocarbon and/or (2) manufacturing cyclic aromatic hydrocarbons such as benzene, toluene, styrene, xylene, ethyl benzene, and cumene made from refined petroleum or liquid hydrocarbons.	321
454312	Liquefied Petroleum Gas Dealers	This U.S. industry comprises establishments primarily engaged in retailing liquefied petroleum (LP) gas via direct selling.	311
11511	Support Activities for Crop Production	This industry comprises establishments primarily engaged in providing support activities for growing crops.	302
311615	Poultry Processing	This U.S. industry comprises establishments primarily engaged in (1) slaughtering poultry and small game and/or (2) preparing processed poultry and small game meat and meat byproducts.	253
1151112	Soil Preparation, Planting, and Cultivating	This U.S. industry comprises establishments primarily engaged in performing a soil preparation activity or crop production service, such as plowing, fertilizing, seed bed preparation, planting, cultivating, and crop protecting services.	207
32512	Industrial Gas Manufacturing	This industry comprises establishments engaged in manufacturing industrial organic and inorganic gases in compressed, liquid, and solid forms.	205

325998	All Other Miscellaneous Chemical Product Manufacturing	This U.S. industry comprises establishments primarily engaged in manufacturing chemical products (except basic chemicals, resins, synthetic rubber; cellulosic and noncellulosic fiber and filaments; pesticides, fertilizers, and other agricultural chemicals; pharmaceuticals and medicines; paints, coatings and adhesives; soap, cleaning compounds, and toilet preparations; printing inks; explosives; custom compounding of purchased resins; and photographic films, papers, plates, and chemicals).	193
325311	Nitrogenous Fertilizer Manufacturing	This U.S. industry comprises establishments primarily engaged in one or more of the following: (1) manufacturing nitrogenous fertilizer materials and mixing ingredients into fertilizers; (2) manufacturing fertilizers from sewage or animal waste; and (3) manufacturing nitrogenous materials and mixing them into fertilizers.	159
49311	General Warehousing and Storage Facilities	This industry comprises establishments primarily engaged in operating merchandise warehousing and storage facilities. These establishments generally handle goods in containers, such as boxes, barrels, and/or drums, using equipment, such as forklifts, pallets, and racks. They are not specialized in handling bulk products of any particular type, size, or quantity of goods or products.	151

Appendix V

DECIDe FRAMEWORK: CRITICAL CHEMICAL INFRASTRUCTURE ADAPTATION

Key Framework Steps

Step 1: Preliminary Investigation

Step 1 involves investigating whether there are overt or covert signs that the group possesses the intent to critical chemical infrastructure. If so, the analysis terminates with a presumption of intent.

Step 2: Data Collection

Step 2 involves the collection of general data on the group and its operating environment. Recommended questions for investigation are listed on page 96.

Step 3: Factor Analysis

Step 3 considers individual framework factors to aid in the final determination of intent regarding target selection. The following general procedure is followed for EACH factor:

i. Each factor analysis begins with the establishment of specific data requirements. When data requirements are met to the extent possible, analysts can proceed directly to step (ii) below.

ii. Where required data is unavailable, analysts should determine the best approximates based on Factor Influences information provided within the framework.

iii. 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.

iv. 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

Step 4 combines the factor analysis information with target space evaluation to arrive at a determination of the existence and strength of the group’s motivation to attack a critical chemical infrastructure target.

DECIDe FRAMEWORK

WORKSHEET

DECIDe FRAMEWORK WORKSHEET

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)*	- . . .

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 CRITICAL CHEMICAL INFRASTRUCTURE *(See Table 5.2)*	MINIMUM ATTACK REQUIREMENTS FOR CI IN GENERAL		OBSERVED / INFERRED TERRORIST GROUP CAPABILITIES
PROTECTION LEVEL	LOW	**HIGH**	**LOW**	
PHYSICAL REQUIREMENTS	MEDIUM	Medium	Low	
WEAPONS	LOW - MEDIUM	Medium	Low - Medium	
FINANCIAL RESOURCES	LOW	Low	Low	
LOGISITICAL RESOURCES	MEDIUM	Medium	Low	
ABILITY TO INNOVATE	MEDIUM	Medium	Low	
TECHNOLOGY LEVEL	LOW - MEDIUM	Medium	Medium	
SKILL SET	MEDIUM	Medium	Medium	
FAMILIARITY w/ TARGET ENVIRONMENT	HIGH	High	Medium	
COMMUNICATIONS	MEDIUM	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

Step 1

PRELIMINARY INVESTIGATION

Data Requirements:

- Is there evidence that the group is planning to attack critical chemical 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 chemical 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. Has the group expressed interest in conducting a CBRN attack or chemical attack, in particular?
2. What level of knowledge does the group have concerning various aspects of the chemical industry, in particular relating to processes and procedures?
3. What does the group perceive the functionality of chemical-related infrastructure to be and how do the view the consequences that might be expected from a successful attack against this type of infrastructure?
4. How has the media recently portrayed the importance and / or vulnerability of chemical-related infrastructure? Are group members likely to have seen these reports?
5. How does the group perceive security around chemical critical infrastructure targets relative to those around other types of infrastructure targets?
6. What level of publicity might the group expect if they successfully attack a chemical CI target?
7. How long has the group existed in its current form (i.e. as a separate organization)?
8. How many generations of members has the group had?
9. What is the observed ideology of the group (including worldview, grand strategic aims and the nature of the perceived enemy)?
10. What is the group's attitude towards human casualties?
11. Which historic events hold symbolic relevance for the group?
12. Is there any evidence of a specific dominant operational objective?
13. What is the size of the group (active members)?
14. Is the organizational structure more centralized (collected in a single geographic region) or more diffuse (for instance, cells scattered over several countries)?
15. Who makes targeting decisions in the group? (autocratic single leader, consultative council, sub-commanders etc.)
16. Does the decision making style tend to be autocratic or consensual?
17. To what extent are leadership decisions carried out?
18. What is the status and position of various factions within the group?
19. What are the demographic characteristics of key group decision makers, especially in terms of education, vocation, and family background?
20. Do any key group decision makers exhibit clear symptoms of psychopathologies that could lead to perceptual impairment?
21. 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?
22. What is the general level of the group's financial resources?
23. How stable/dependable are current sources of financial resources and what is the cost to the group to obtain them?
24. What kinds and amounts of physical resources (weapons, equipment, vehicles, etc.) does the group possess?
25. 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?
26. What type of security environment does the group face at the time of target selection?
27. How vulnerable is the group to detection, infiltration and elimination by the security forces of their opponents?
28. Do group decision makers have a set timetable for action?
29. Does the group currently perceive itself to be under threat?
30. What is the group's history of innovation (both tactically and technically)?
31. What is the group's general technological level?
32. 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)?
33. How familiar is the group with the general target environment?
34. 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?
35. Which external groups do the terrorist decision makers perceive as opponents?
36. What is the level of publicity terrorists expect from different media groupings?
37. 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?
38. How has the media recently portrayed critical infrastructure?
39. 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?
40. What is the level of publicity they expect to receive by attacking various targets?
41. How tolerant are decision makers about risk (in terms of operational success, group survivability and the welfare of group members)?

Step 3

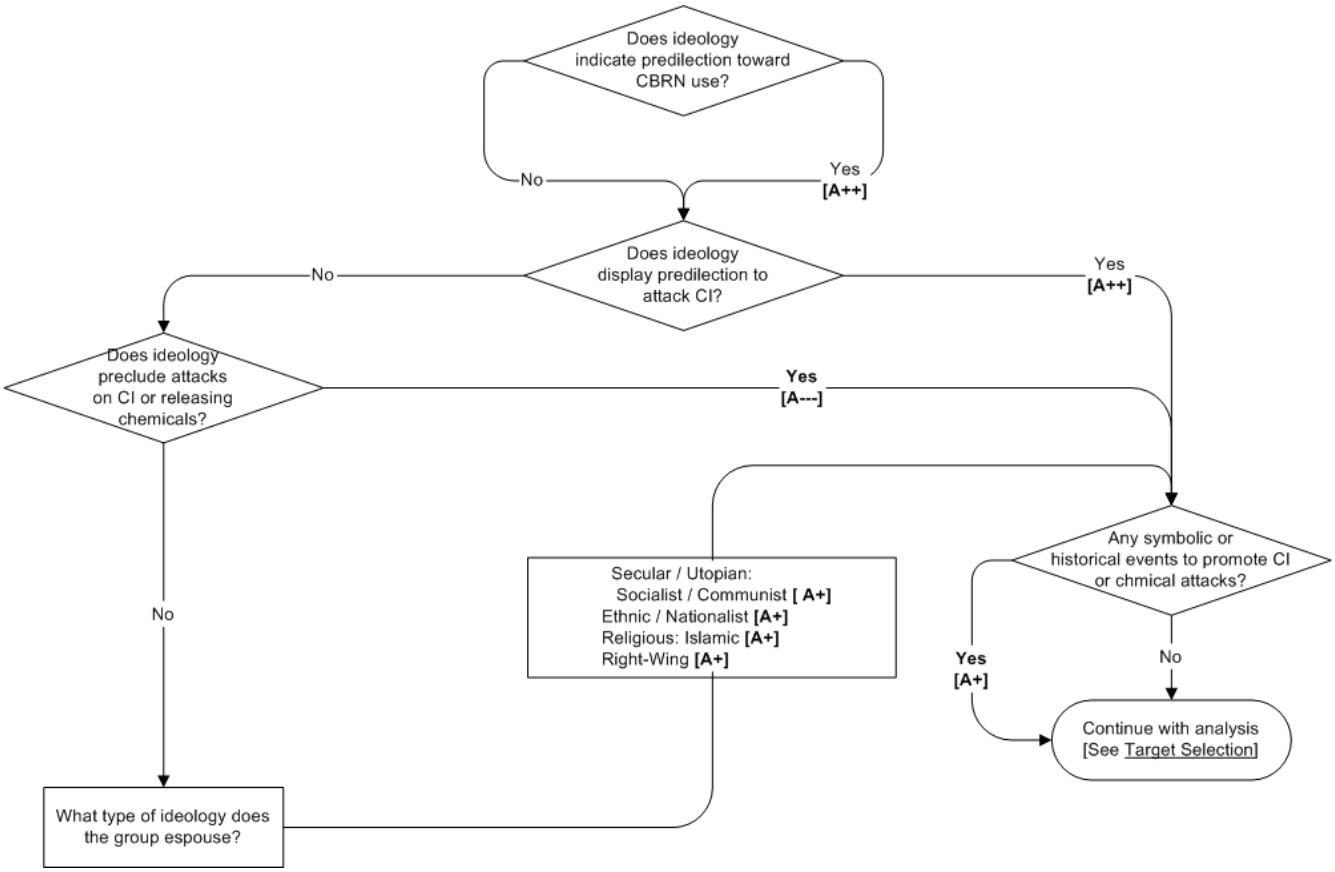
FACTOR ANALYSIS

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]

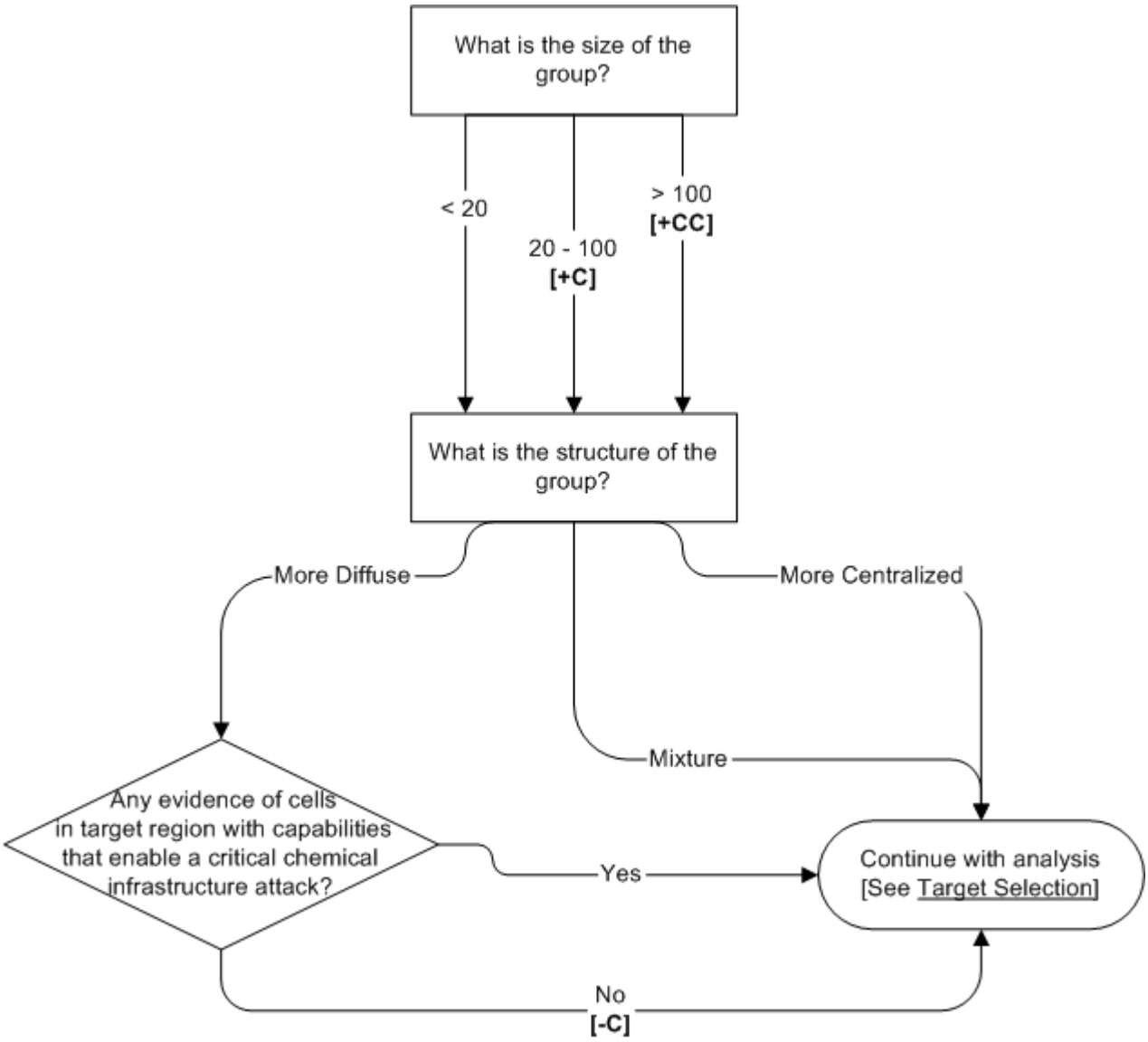


Factor Analysis: Organizational Structure

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]



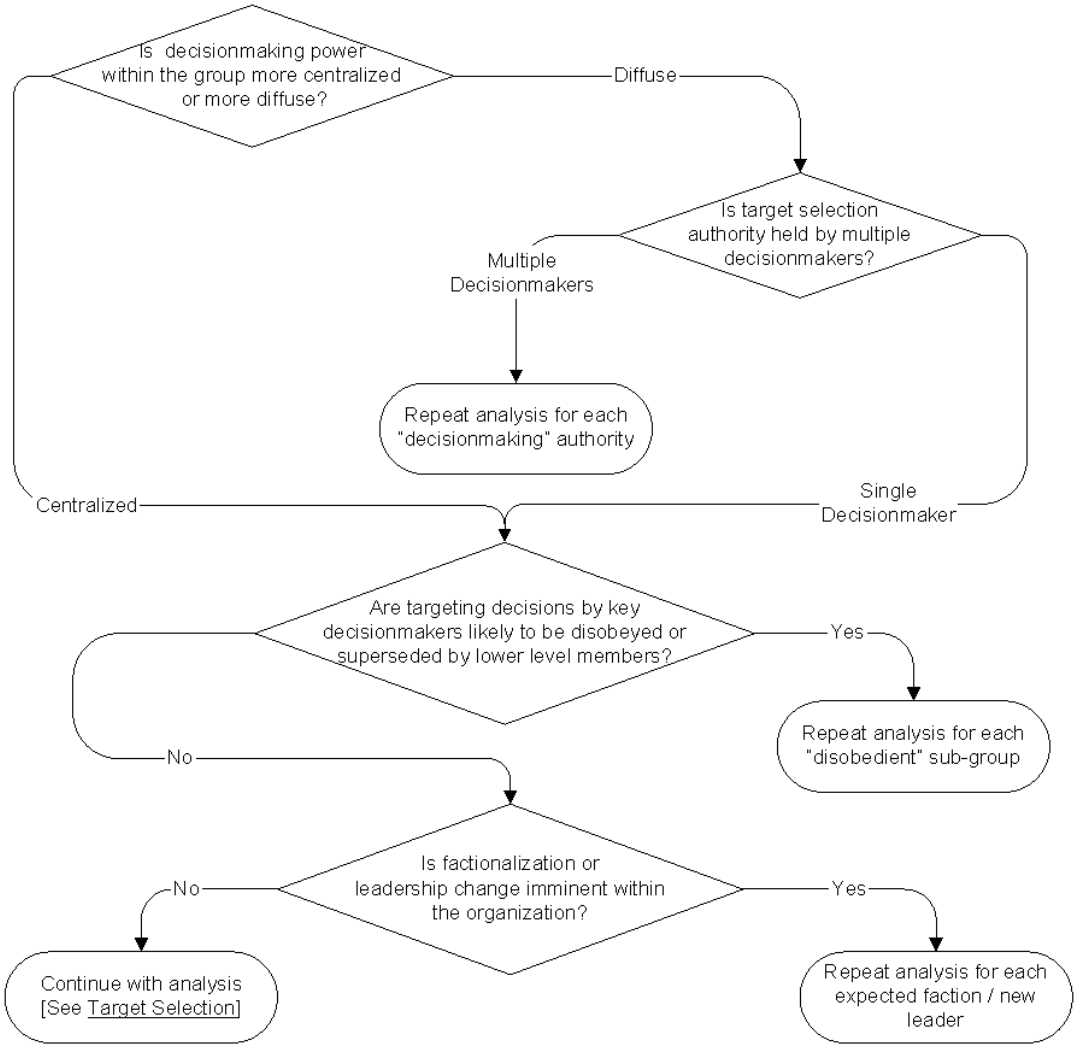
Factor Analysis: Organizational Dynamics

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.



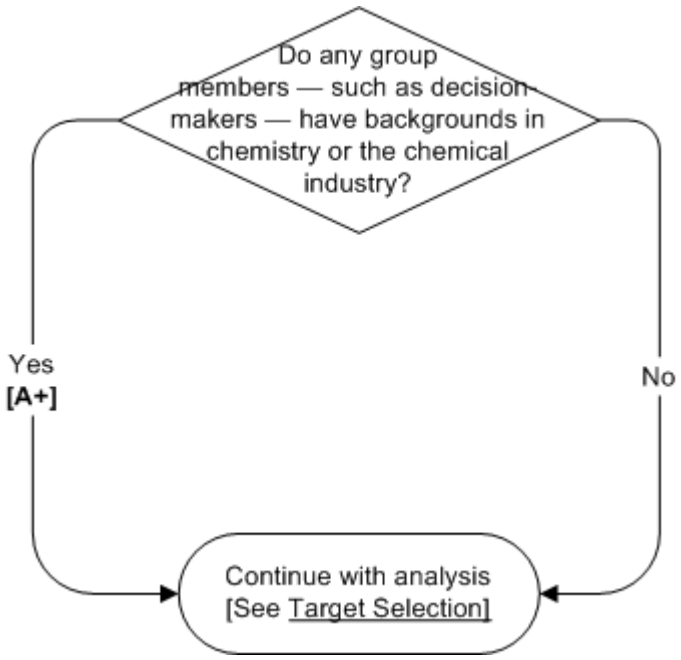
Factor Analysis: Demographics

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.*



Factor Analysis: Resources

Data Requirements:

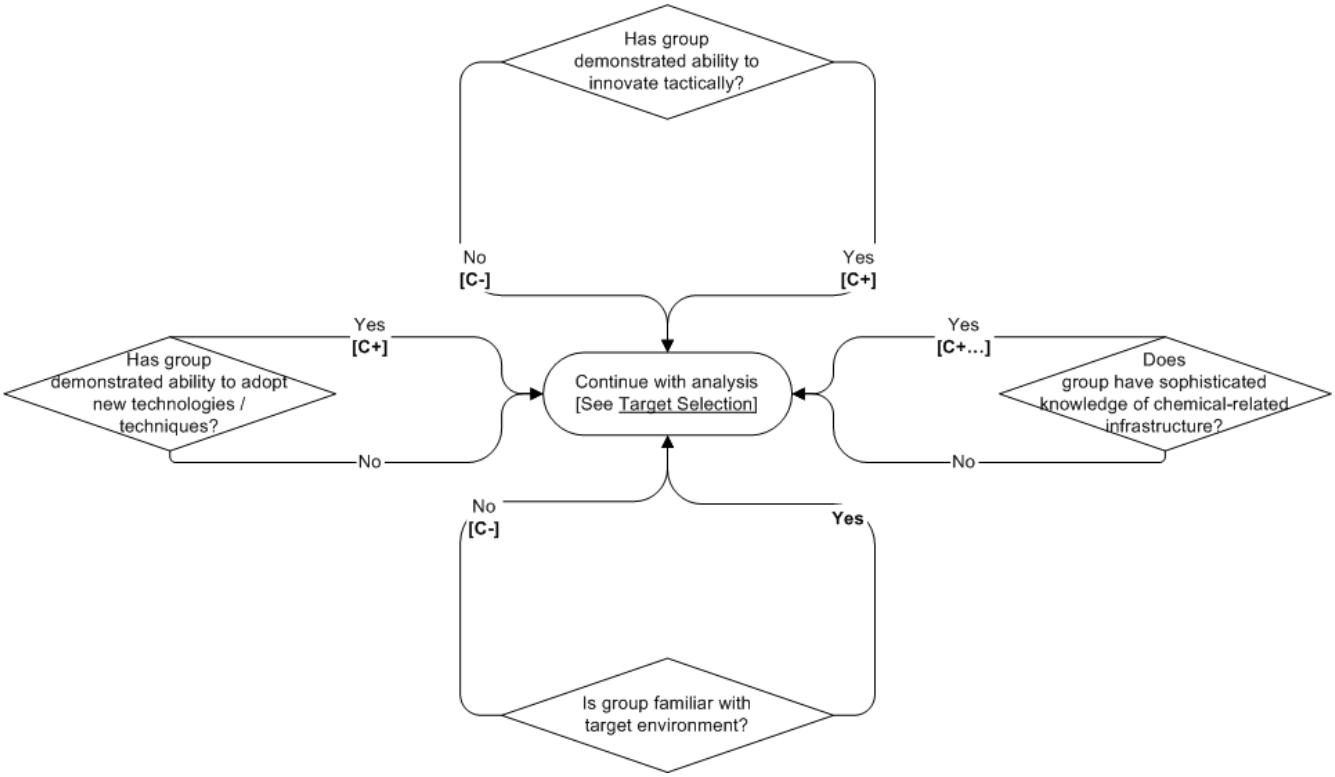
- What is the general level of the group's financial resources?
- How stable/dependable are current sources of financial resources and what is the cost to the group to obtain them?
- What kinds and amounts of physical resources (weapons, equipment, vehicles, etc.) does the group possess?
- How expansive 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 Analysis: Operational Capabilities

Data Requirements:

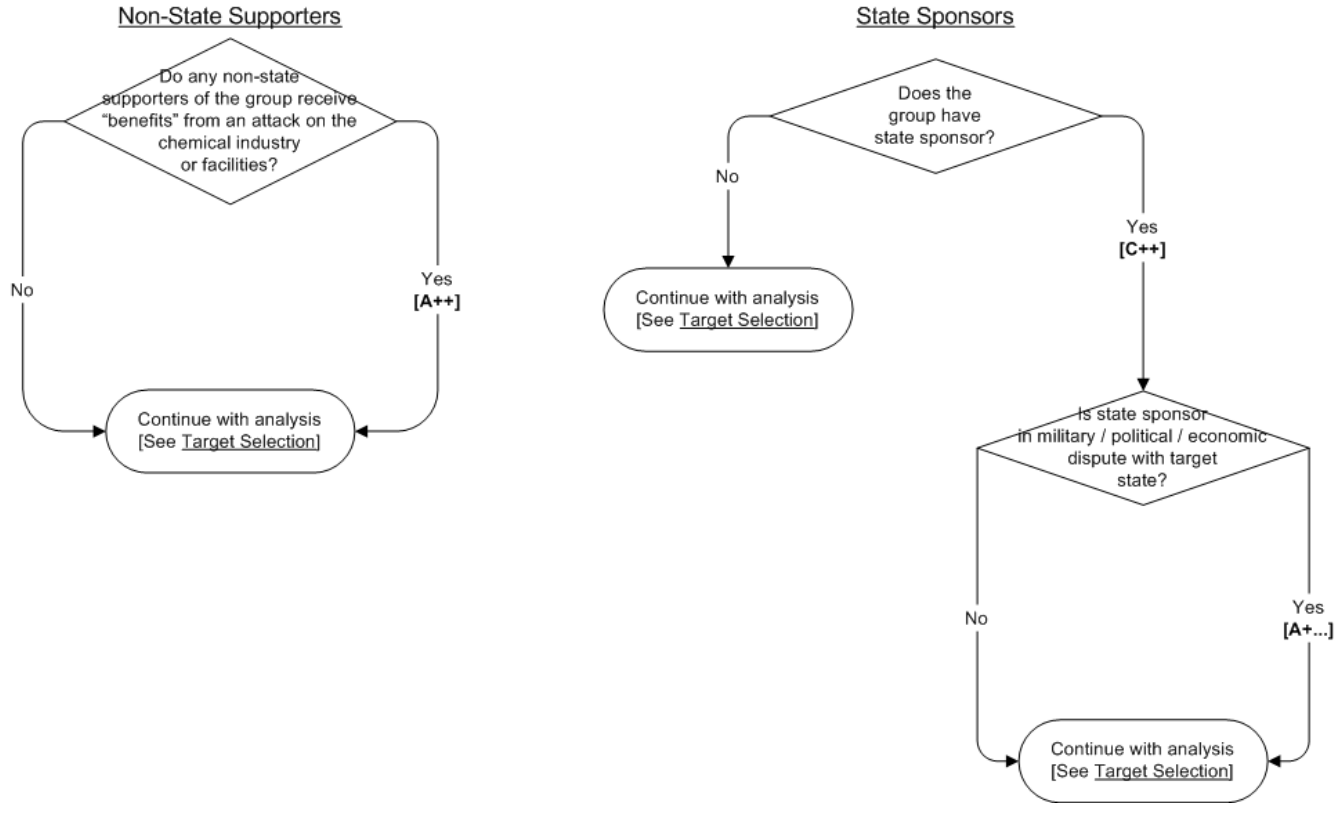
- What is the group's history of innovation (both tactically and technically)?
- What is the group's general technological level?
- What is the group's knowledge level of chemical-related infrastructure?
- How familiar is the group with the target environment?



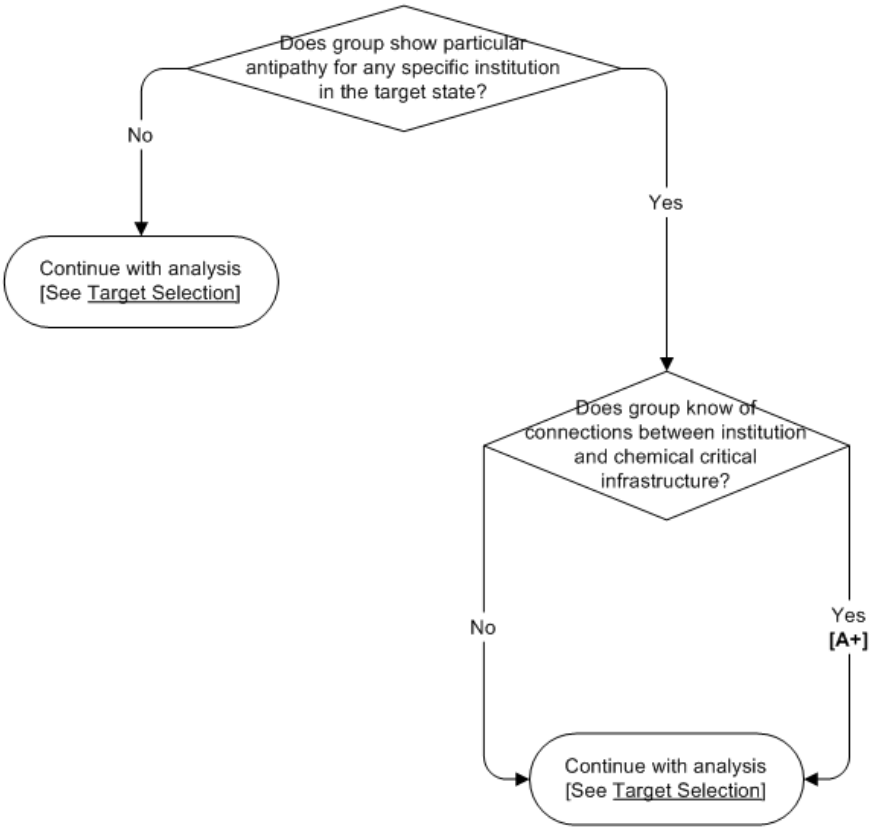
Factor Analysis: External Relations

Data Requirements:

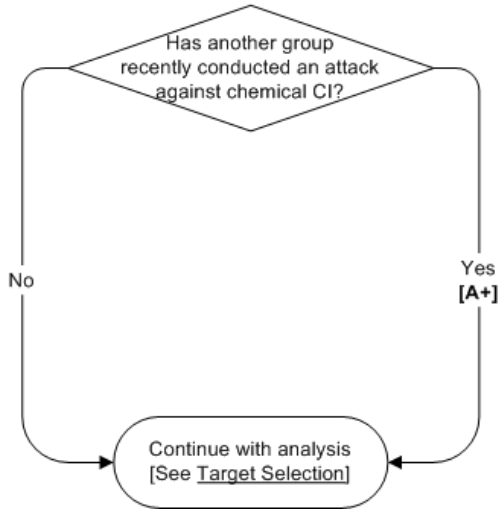
- Which external groups or organizations do the terrorist decision makers perceive as allies or potential allies?
- Of these, the support of which external groups or organizations do they seek to gain or maintain?
- Which external groups do the terrorist decision makers perceive as opponents?
- What is the level of publicity terrorists expect from different media groupings?
- How has the media recently portrayed critical infrastructure?



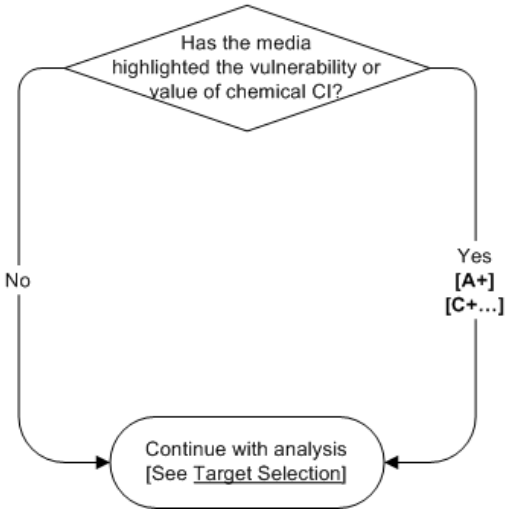
State Apparatus



Other Groups



Media



Factor Analysis: Critical Infrastructure Characteristics

Data Requirements:

- What is the level of protection decision makers perceive critical chemical infrastructure targets in general (relative to other targets) have?
- What does the group perceive the functionality of the target to be and the consequences they expect from a successful attack against the critical chemical infrastructure target?*
- What is the level of publicity they expect to receive by attacking that particular target?

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.

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?

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.

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 chemical 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 chemical infrastructure attacks in this case are not necessarily against critical chemical infrastructure, but against any types of related 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[181]. 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 chemical 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 chemical 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 chemical infrastructure in a developed country like the United States is less necessary and the attractiveness of a high-impact critical chemical infrastructure target decreases.

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 fact 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 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 chemical CI attacks are not excluded or prescribed.

[181] Of course, any category CAN have a desired symbolic effect, even if it is not necessary.

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[182][found in the second section of Table AV-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[183]? [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. It should be noted that chemical CI targets offer some of the few critical infrastructure targets that are capable of causing catastrophic casualties. Therefore, if a group wants to cause massive economic damage, major disruption (including psychological impact), and large numbers of casualties, critical chemical infrastructure could be a desirable target for the group.

Mitigating Factors:

Is the group dependent upon or does it perceive benefits from certain types of critical chemical infrastructure in its target area[184]?
If so, then those particular types of chemical CI will likely be excluded from the target set. It should be noted, however, that terrorists are likely to be less immediately dependent on chemicals, than on infrastructures such as water, power, and transportation. If a group has a major base, constituency population or vital resources in an area that could be contaminated by a successful chemical CI attack, it is likely to select an alternate target. Additionally, the "uncontrollability" – in terms of never being able to control for factors such as weather – may make critical chemical infrastructure attacks less desirable in the eyes of some terrorists.

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 chemical infrastructure targets.

---

[182] 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 chemical infrastructure.
[183] 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.
[184] 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 chemical infrastructure targets that group decision makers could perceive as generating an especially high degree of publicity?

If YES, this means that critical chemical infrastructure is in the restricted target set. An attack truly intended to cripple such critical infrastructure is automatically a terrorist 'spectacular'.

2. Bearing in mind the progressive restriction of target space process, use Table AV-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 chemical 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 chemical CI targets remain in the target set and, in some cases, inform the analyst whether or not critical chemical infrastructure is the only element left in the likely target set.

Capabilities Analysis[185]

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,[186] 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[187]. 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'[188] 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.

---

[185] In this section 'capabilities' refers to both resources and operational capabilities.
[186] 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.
[187] 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.
[188] 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[189].

[189] 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 A-V.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 FACILITY	**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

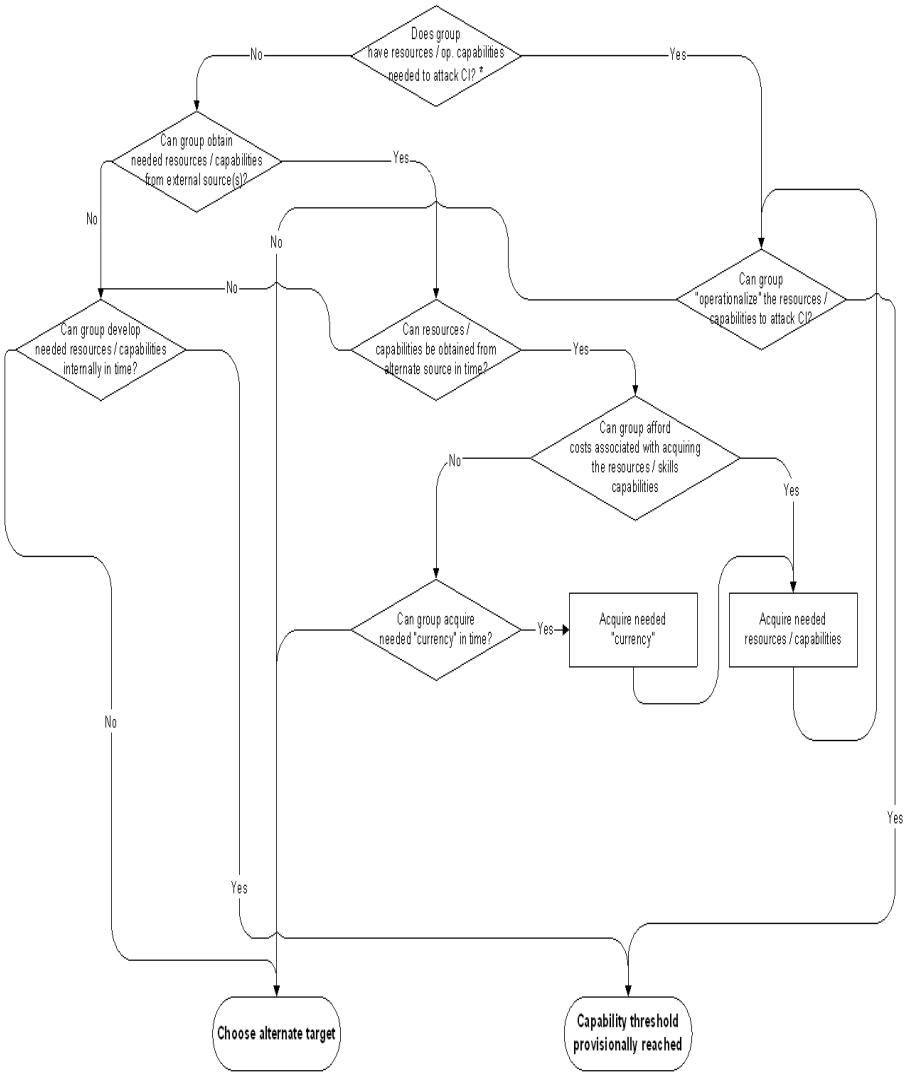
Ability to innovate:
High: Easily embraces new technologies and techniques; quickly gains tacit knowledge
Medium: Competent at adopting new technologies and techniques, although not a particular strength
Low: Difficulty adopting new technologies or techniques

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."[190]

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[191]:

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[192] 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.
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

[190] Bruce Schneier, *Secrets and Lies: Digital Security in the Networked World* (Wiley Publishing, Inc., 2004), p.48.
[191] 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."
[192] In many cases, the target set may contain only a single member. 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, p. 13. <http://www.ciaonet.org/wps/hob03/>.

their decision process again (or at least several factors of the process) in order to select an alternative target.[193]

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[194] 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[195]. 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.

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

[193] 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.
[194] 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.
[195] See Chapter 2 for a detailed discussion of the effect of target characteristics on target selection.

information. Also, the attractiveness values need to be considered, not in isolation, but relative to the attractiveness of other target and attack types[196]. 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.

[196] 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.