



START

Terrorist Attacks Targeting Critical Infrastructure in the United States, 1970-2015

*Report to the Office of Intelligence and Analysis,
U.S. Department of Homeland Security*

June 2016

National Consortium for the Study of Terrorism and Responses to Terrorism
A Department of Homeland Security Science and Technology Center of Excellence
Based at the University of Maryland

8400 Baltimore Ave, Suite 250 • College Park, MD 20740 • 301.405.6600

www.start.umd.edu

About This Report

The author of this report is Erin Miller at the University of Maryland. Questions about this report should be directed to Erin Miller at eemiller@umd.edu.

This research was supported by the U.S. Department of Homeland Security through Award Number 2012-ST-061-CS0001-04-AMENDMENT 4. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security or START.

The initial collection of data for the Global Terrorism Database (GTD) data was carried out by the Pinkerton Global Intelligence Services (PGIS) between 1970 and 1997 and was donated to the University of Maryland in 2001. Digitizing and validating the original GTD data from 1970 to 1997 was funded by a grant from the National Institute of Justice in 2004 (PIs Gary LaFree and Laura Dugan; grant number: NIJ2002-DT-CX-0001) and in 2005 as part of the START Center of Excellence by the Department of Homeland Security Science and Technology Directorate (DHS S&T), Office of University Programs (PI Gary LaFree; grant numbers N00140510629 and 2008-ST-061-ST0004). Data collection for incidents that occurred between January 1998 and March 2008 and updates to the earlier data to make it consistent with new GTD coding criteria were funded by the DHS S&T Human Factors/Behavioral Sciences Division (HFD) (PIs Gary LaFree and Gary Ackerman; contract number HSHQDC-05-X-00482) and conducted by database staff at the National Consortium for the Study of Terrorism and Responses to Terrorism (START) and the Center for Terrorism and Intelligence Studies (CETIS). For GTD data collection from April 2008 to October 2011, START partnered with the Institute for the Study of Violent Groups (ISVG), headquartered at New Haven University. These efforts were funded by a grant from DHS S&T Office of University Programs, (PI Gary LaFree; grant number 2008-ST-061-ST0004).

Beginning with events that occurred in November 2011, the START Consortium headquartered at the University of Maryland began collecting all data for the GTD independently. Since then, all GTD collection has been jointly funded by DHS S&T Office of University Programs (PI Gary LaFree; grant number 2012-ST-061-CS0001) and by the U.S. State Department (PIs Gary LaFree and Erin Miller; contract number SAQMMA12M1292). The GTD now includes information on 141,966 terrorist attacks from around the world from 1970 through 2014 and can be accessed directly from the START [website](#).

In addition to ongoing data collection, efforts to review and update information on terrorist attacks in the United States have been supported through funding from the DHS S&T Resilient Systems Division (PI Gary LaFree, grant number # 2009ST108LR0003). Beginning in 2009, efforts to supplement GTD data for the United States have included systematically reviewing numerous chronologies of terrorism and political violence to identify cases that qualify for inclusion in the GTD, as well as updating existing GTD cases with new information. This report focuses on the U.S. segment of the Global Terrorism Database.

About START

The National Consortium for the Study of Terrorism and Responses to Terrorism (START) is supported in part by the Science and Technology Directorate of the U.S. Department of Homeland Security through a Center of Excellence program based at the University of Maryland. START uses state-of-the-art theories, methods and data from the social and behavioral sciences to improve understanding of the origins, dynamics and social and psychological impacts of terrorism. For more information, contact START at infostart@start.umd.edu or visit www.start.umd.edu.

Citations

To cite this report, please use this format:

Miller, Erin. Terrorist Attacks Targeting Critical Infrastructure in the United States, 1970-2015. College Park, MD: START, 2016.

Contents

Introduction	1
Data Collection Methodology.....	1
Processing GTD Source Documents	2
Defining Terrorism.....	2
GTD Variables and Coding.....	3
Methodological Consistency.....	3
Critical Infrastructure Classification and Limitations.....	4
Profiles of Perpetrators of Terrorism in the United States (PPT-US)	5
Terrorist Attacks on Critical Infrastructure in the United States	6
Attack Patterns and Lethality	6
Terrorist Attacks on Critical Infrastructure Sectors.....	8
Commercial Facilities Sector	8
Government Facilities Sector	10
Healthcare and Public Health Sector	11
Financial Services Sector	13
Defense Industrial Base Sector.....	14
Emergency Services Sector	15
Energy Sector	16
Transportation Systems Sector.....	17
Food and Agriculture Sector.....	19
Other Sectors.....	20
Conclusions.....	20

Introduction

This report leverages the Global Terrorism Database (GTD) to provide an overview of terrorist threats to critical infrastructure in the United States based on patterns of terrorism from 1970 to 2015. First, I identify trends in terrorist attacks targeting critical infrastructure in the United States, compared to terrorist attacks against other types of targets. Next, I identify the most commonly targeted types of critical infrastructure in the United States. Throughout this analysis, I highlight the perpetrator organizations that have historically targeted critical infrastructure in the United States, referencing the Profiles of Perpetrators of Terrorism in the United States (PPT-US) to provide additional context about these groups. In addition, for each of the critical infrastructure sectors most impacted by terrorist attacks, I describe the tactics and weapons typically used.

The purpose of this report is to provide a general understanding of the potential threats terrorism poses to critical infrastructure in the United States, serving as a foundation for generating questions for future research. Thus, I conclude with a brief discussion of topics that may be of interest for more in-depth analysis. Before presenting the results, I begin with an overview of the data collection methodology for the datasets referenced to produce this report.

Data Collection Methodology¹

The Global Terrorism Database is the result of multiple data collection efforts carried out since 1970 that have relied on publicly available, unclassified source materials, mainly media articles and electronic news archives. The data that originally comprised the core of the GTD from 1970 to 1997 were collected by Pinkerton Global Intelligence Services (PGIS) on handwritten index cards. Beginning in 2001, a team of researchers at the University of Maryland obtained these original records and digitized them. By 2006 the maintenance of this dataset had become a key component of the research portfolio developed by the National Consortium for the Study of Terrorism and Responses to Terrorism (START), and the GTD team began partnering with other organizations to carry out ongoing data collection for events that took place after 1997. Throughout this period, START researchers conducted supplemental data collection projects to systematically compare the GTD to other sources of data to improve its completeness and worked to update historical event details when possible. In 2012, the GTD team at START moved the primary data collection effort to START headquarters at the University of Maryland. Since then, START has assumed sole responsibility for all aspects of the collection and maintenance of the GTD. To accomplish this, we developed an innovative data collection methodology for the GTD that is based on more than 10 years of experience and lessons learned with respect to the complexities and challenges of systematically collecting valid data on terrorist attacks worldwide.

¹ Parts of this section were excerpted from the following reports:

Miller, Erin. Profiles of Perpetrators of Terrorism in the United States, 1970-2013: Final Report to Resilient Systems Division, DHS Science and Technology Directorate. College Park, MD: START, 2014.

Miller, Erin. Patterns of Terrorism in the United States, 1970-2014. College Park, MD: START, 2015.

Additional information about the data collection methodology can be found on the GTD [website](#) and in the GTD [codebook](#).

Processing GTD Source Documents

Within the evolving framework of news media and technology, START's objective is to enhance the efficiency, accuracy, and completeness of GTD collection. We accomplish this by combining the strengths of both automated and manual techniques. The data collection process draws on more than one million media articles on any topic published daily worldwide. The process of identifying the relatively small subset of these articles that describe terrorist attacks begins with applying customized keyword filters to the "fire hose" of media articles available through a subscription to the Metabase Application Programming Interface (API) provided by Moreover Technologies, Inc. We supplement the English-language content from Metabase with articles downloaded from the Open Source Center (www.opensource.gov), which includes English-language translations of sources from more than 160 countries in more than 80 languages. The initial filters isolate a pool of potentially relevant articles, approximately 200,000 per month. We reduce this subset using more sophisticated natural language processing and machine learning techniques to remove duplicates and score the likely relevance of the articles. The GTD team manually reviews this second subset of articles, approximately 20,000 each month, to identify the unique events that satisfy the GTD inclusion criteria. Finally, the coding team reads the articles that are linked to specific events and records the details of each event according to the specifications of the GTD Codebook.

Defining Terrorism

The GTD defines terrorism as "the threatened or actual use of illegal force and violence by a non-state actor to achieve a political, economic, religious, or social goal through fear, coercion, or intimidation."² To operationalize this definition, GTD researchers include in the database those incidents that satisfy each of the following mandatory inclusion criteria:

- The incident must be intentional, i.e., the result of a conscious calculation on the part of a perpetrator.
- The incident must entail some level of violence or threat of violence, including property violence as well as violence against people.
- The perpetrators of the incidents must be sub-national actors. The database does not include acts of state terrorism.

In addition, incidents recorded in the GTD must meet *at least two* of the following inclusion criteria:

1. The act must be aimed at attaining a political, economic, religious, or social goal.
2. There must be evidence of an intention to coerce, intimidate, or convey some other message to a larger audience (or audiences) than the immediate victims.
3. The action must be outside the precepts of International Humanitarian Law insofar as it targets non-combatants.

Given that it can be difficult to unambiguously determine if an event satisfies these inclusion criteria, the GTD records also include a variable indicating whether or not there is specific doubt that the inclusion

² National Consortium for the Study of Terrorism and Responses to Terrorism (START). (2015, June). Global Terrorism Database: Codebook. Retrieved May 11, 2016, from <https://www.start.umd.edu/gtd/downloads/Codebook.pdf>

criteria are satisfied. Such doubt is typically a result of incomplete or conflicting reports about the circumstances of the attack. These attacks are included in the analysis presented in this report. In addition, inclusion in the GTD requires that some kinetic action has been taken on the part of the perpetrators to carry out the attack. We informally refer to this as the “out the door” rule, in that the perpetrators must be on their way to carry out the attack to be included in the GTD. Once the perpetrators are “out the door,” if the attack fails or is otherwise thwarted we include it in the database and mark it as unsuccessful. The GTD does not include plots, conspiracies, or hoaxes that were not actually attempted. The GTD does not include violence that occurs spontaneously, such as rioting or violence precipitated by the actions of authorities (e.g., police raid, traffic stop, or arrest). The GTD also does not include non-violent activity such as peaceful protests, vandalism, or civil disobedience.

GTD Variables and Coding

The GTD coding strategy relies on six coding teams that each specializes on a particular domain of the GTD Codebook. The domains include location, perpetrators, targets, weapons and tactics, casualties and consequences, and general information. Each team is comprised of three to six undergraduate or graduate student interns led by a research assistant and is responsible for coding the domain-specific variables for each event in the GTD. The domain team leaders are responsible for the training and supervision of team members and ensuring the quality of the coded data. This approach guarantees that each piece of information is coded and reviewed by someone who is familiar with the particular coding guidelines for the domain, as well as the relevant context. For example, the perpetrator domain team will have greater familiarity with active perpetrator organizations, their naming conventions, aliases, spelling variations, factions, and splinter organizations, making them well-suited to systematically record information on the organizations attributed responsibility for an attack.

Methodological Consistency

Although the data collection process recently developed at the University of Maryland has improved the internal consistency and comprehensiveness of the GTD, as with any shift in data collection methodology it is critical to recognize the implications for analysis. The first year of data collected under the new process, 2012, represents a nearly 70 percent increase in the total number of worldwide terrorist attacks over 2011. The magnitude of this change is far from uniform across countries and the increase likely reflects recent patterns of terrorism in certain locations. However, it is also partly a result of the improved efficiency of the data collection process. The ongoing rapid growth of the internet, and news archives and aggregators in particular, makes a product like Metabase available to researchers, implicitly improving access to a greater variety of national and local sources. The use of automated approaches to document classification allows the GTD team to focus more time reviewing only those source articles that are classified as “relevant” by machine learning algorithms.

As a result, we have the resources to leverage a much broader and deeper pool of media sources from around the world. Despite consistency in our definition of terrorism and inclusion criteria, this exponential growth in available source materials has allowed us to collect more comprehensive data on terrorism than any previous effort. The GTD research team will continue to evaluate the impact of source availability on trends in the database to better advise users on important implications for analysis. We

will also continue to work to supplement the GTD “legacy” data on terrorist attacks since 1970 to further improve its completeness. In general, comparisons of aggregate statistics over time and between locations—and their implications for the state of international security and global counterterrorism efforts—should be interpreted with caution due to considerable variation in the availability of source materials.

However, because the availability of source information pertaining to the United States has always been relatively robust, and the GTD team has conducted extensive supplemental data collection efforts for incidents occurring in the United States, we expect that the methodological artifacts described here have a minimal impact on analysis described in this report. In fact, data from 1993 are typically not included in the GTD because the original records were lost in an office move before the data were transferred to START. However, the supplemental data for terrorist attacks the United States in 1993 are sufficiently robust and are included in the statistics in this report. Collection and revision of the data are ongoing, and the exact numbers of attacks presented in this report may change slightly as new data become available.

Critical Infrastructure Classification and Limitations

The classification of targets based on the critical infrastructure sectors recognized by the Department of Homeland Security is not part of the general GTD collection process. The GTD does include a target classification scheme that identifies the type of target attacked, based 21 different categories of targets that do not directly align with the critical infrastructure sectors. (See Table 1 for a listing of the GTD target types and the critical infrastructure sectors identified by Presidential Policy Directive 21: Critical Infrastructure Security and Resilience). As part of the development of the Integrated United States Security Database (IUSSD) project, analysts at START reviewed all attacks recorded in the GTD that occurred in the United States and classified them based on the critical infrastructure sectors using available target descriptors. For many of the terrorist attacks in the United States, this classification process was relatively straightforward. For example, attacks against entities classified as airports and aircraft, maritime, or transportation targets in the GTD correspond to the Transportation Systems Sector. However, targets that were categorized as businesses using the GTD classification scheme may fit most appropriately in the Commercial Facilities Sector, the Financial Services Sector, or the Food and Agriculture Sector, among others. Finally, certain types of targets recognized in the GTD represent entities that do not qualify as types of critical infrastructure. These included most commonly: private citizens and property, educational institutions, religious figures and institutions, and journalists and media.

Our efforts to classify targets based on the critical infrastructure sectors accommodated only one sector per attack, which for the most part was sufficient. Less than 4 percent of all attacks that took place in the United States involved more than one target. However, there were a small number of attacks for which this practice presents a limitation. For example, the four attacks on September 11, 2001 each conceivably targeted multiple critical infrastructure sectors, including the Commercial Facilities Sector, the Defense Industrial Base Sector, the Financial Services Sector, the Government Facilities Sector, and the Transportation Systems Sector. Although perhaps not directly targeted, other sectors were certainly impacted by these attacks as well, including most notably the Emergency Services Sector. Note that we

classified the September 11th attack in which a hijacked commercial aircraft crashed into the Pentagon as an attack on the Defense Industrial Base Sector, and we classified those in which hijacked commercial aircraft crashed in New York City and near Shanksville, Pennsylvania as attacks on the Transportation Systems Sector.

Table 1: GTD Target Types and Critical Infrastructure Sectors

GTD Target Types	Critical Infrastructure Sectors
Abortion Related	Chemical Sector
Airports & Aircraft	Commercial Facilities Sector
Business	Communications Sector
Educational Institution	Critical Manufacturing Sector
Food or Water Supply	Dams Sector
Government (Diplomatic)	Defense Industrial Base Sector
Government (Non-Diplomatic)	Emergency Services Sector
Journalists & Media	Energy Sector
Maritime Vessels	Financial Services Sector
Military	Food and Agriculture Sector
NGO	Government Facilities Sector
Other	Healthcare and Public Health Sector
Police	Information Technology Sector
Private Citizens & Property	Nuclear Reactors, Materials, and Waste Sector
Religious Figures/Institutions	Transportation Systems Sector
Telecommunication Systems	Water and Wastewater Systems Sector
Terrorists/Non-State Militia	
Tourists	
Transportation	
Utilities	
Violent Political Party	

Profiles of Perpetrators of Terrorism in the United States (PPT-US)

Profiles of Perpetrators of Terrorism in the United States (PPT-US) is a comprehensive dataset including structured data collected from unclassified sources on 143 organizations that carried out terrorist attacks in the United States between 1970 and 2015. The database contains more than 100 variables pertaining to the organizations’ historical contexts and philosophical motivations, ideologies, goals, operations, structures, and funding sources. PPT-US also includes references to source materials and confidence levels for each data point to allow users to better assess the validity of information that is often difficult to verify. The PPT-US data and supporting documentation are made available to the public to provide analysts with a resource for investigating the characteristics of perpetrator groups that have carried out terrorist attacks in the United States.

Groups are included in PPT-US if they have conducted at least one terrorist attack in the United States (including Puerto Rico) since 1970 based on the definition of terrorism used in the GTD. That is, any

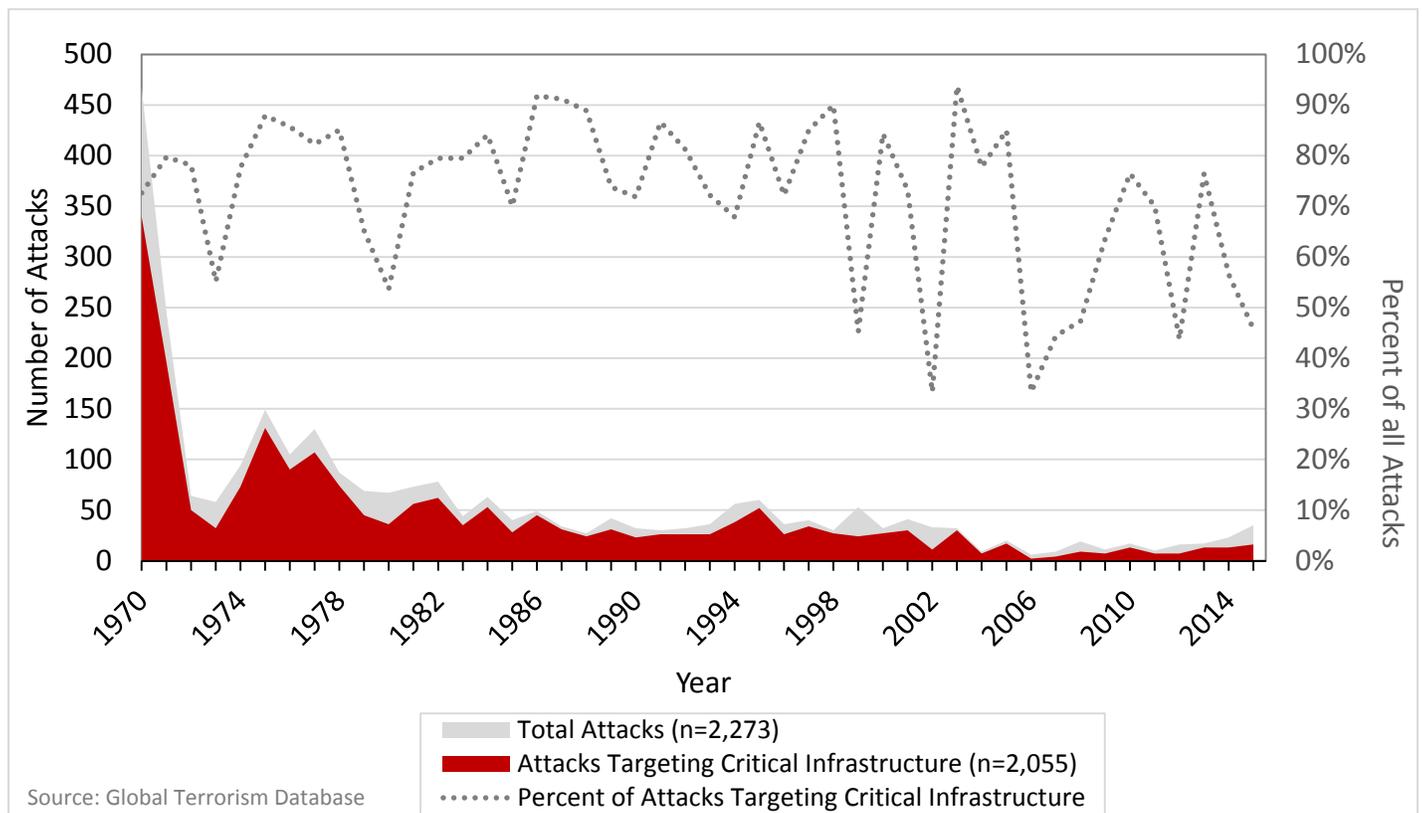
group identified in the GTD as a perpetrator of an attack targeting the U.S. homeland is included in PPT-US. Note that groups thought to be suspicious, dangerous, or known to espouse extremist ideology but that have never carried out a terrorist attack against the United States are omitted from PPT-US. Also PPT-US includes only named organizations. Individual perpetrators of terrorist attacks not affiliated with a named organization are not included in the dataset. Finally, groups that have targeted U.S. interests abroad, but not carried out attacks on U.S. soil, are not included.

Additional criteria were developed for including an organization in PPT-US: First, the GTD includes a variable that indicates if there is uncertainty among the coders about whether that incident should be classified as terrorism or, instead, whether it would be more properly classified as another type of violence (e.g., insurgency, inter- or intra-group conflict, or conventional crime). If such uncertainty exists for all of a particular group’s activities, the group is excluded from PPT. In addition, when attributing responsibility for specific incidents in the GTD to organizations, the GTD team records whether there is high confidence that an organization is, in fact, responsible for the attack or, conversely, whether the group is only the suspected perpetrator. Only GTD groups for which there is high confidence of responsibility for at least one attack are included in PPT-US. By applying these selection criteria, 143 groups responsible for more than 1,250 terrorist attacks in the United States between 1970 and 2015 are included in PPT-US.

Terrorist Attacks on Critical Infrastructure in the United States

Attack Patterns and Lethality

Figure 1: Total terrorist attacks and attacks targeting critical infrastructure in the United States by year, 1970-2015



Between 1970 and 2015, 2,723 terrorist attacks took place in the United States, causing a total of 3,570 deaths; of these, 2,055 attacks (75%) targeted critical infrastructure. Figure 1 illustrates that the pattern of attacks that targeted critical infrastructure was consistent with the pattern of attacks overall. That is, the frequency of attacks was highest in the 1970s—in particular, one-third (34%) of all attacks on critical infrastructure took place between 1970 and 1974—and declined gradually throughout the 1980s, 1990s, and 2000s.

The 668 terrorist attacks that did not target critical infrastructure involved a variety of target types, but most frequently these targets were classified as private citizens and property (38%), educational institutions (24%), religious figures and institutions (16%), and journalist and media (9%).

The impact of terrorist attacks on critical infrastructure is inherently disruptive; however, the lethality of these attacks also closely mirrored the lethality of attacks in the United States more generally. In particular, the vast majority of terrorist attacks in the United States between 1970 and 2015 were non-lethal, with a few exceptions in which attacks were extraordinarily deadly. In fact, 89 percent of all deaths due to terrorist attacks in the United States during this time period were caused by the 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City (5%) and the September 11, 2001 attacks (84%).

Terrorist attacks on critical infrastructure were also paradoxically less likely to be deadly and more likely to be *highly* deadly than attacks that did not target critical infrastructure. As shown in Table 2, more than 90 percent of all attacks that targeted critical infrastructure were non-lethal, compared to just over 80 percent of attacks that did not target critical infrastructure. In contrast, 15 percent of attacks that did not target critical infrastructure resulted in a single death, compared to 5 percent of attacks that did target critical infrastructure.

Table 2: Lethality of Terrorist Attacks in the United States, 1970-2015

Total Number of Deaths	Attacks Targeting Critical Infrastructure		Attacks Not Targeting Critical Infrastructure	
	Number	Percent	Number	Percent
0	1854	93.3%	534	81.5%
1	90	4.5%	96	14.7%
2-4	31	1.6%	20	3.1%
5-10	4	0.2%	4	0.6%
11-150	4	0.2%	1	0.1%
>150	4	0.2%	0	0.0%
Total	1986	100.00%	655	100.00%

Note: Total number of deaths is unknown for 3% of all attacks in the United States.

Source: Global Terrorism Database

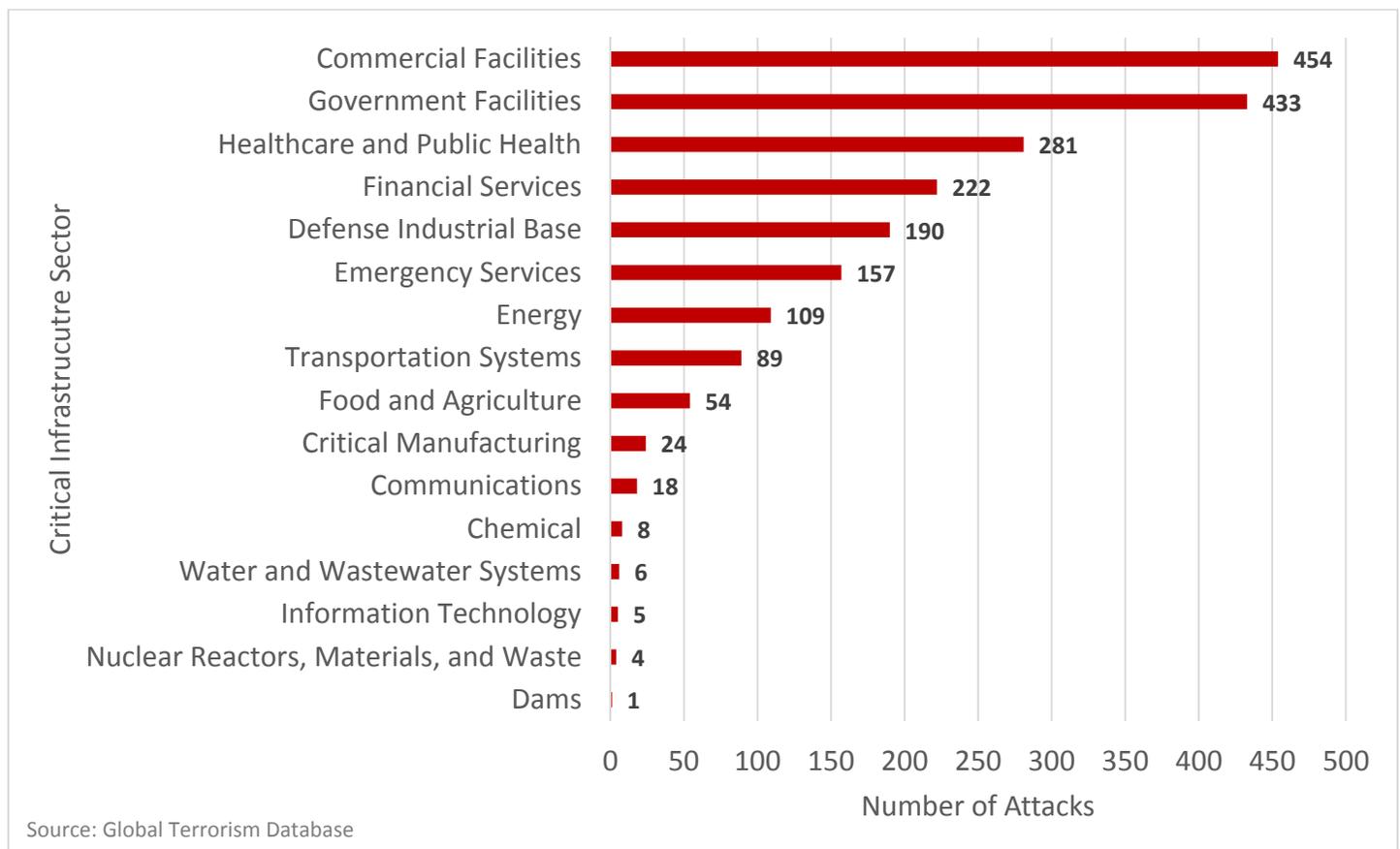
There are a number of reasons an attack may be non-lethal, including the possibility that it was attempted, but unsuccessful—either the attack failed on its own or was thwarted by others. In other cases the attack was not intended to be deadly, but instead to cause property damage rather than loss of

life. In light of this, the discrepancy here between attacks that targeted critical infrastructure and those that did not may reflect a tendency for attacks against private citizens and property, educational institutions, religious figures and institutions, and journalists and the media to target specific individuals rather than buildings or places where large numbers of people congregate. Although relatively few attacks overall resulted in more than 10 deaths, those that did were disproportionately likely to target critical infrastructure.

Terrorist Attacks on Critical Infrastructure Sectors

Among the terrorist attacks that did target critical infrastructure, certain sectors were impacted more than others. Between 1970 and 2015, more than two-thirds (68%) of all attacks on critical infrastructure in the United States targeted the commercial facilities (22%), government facilities (21%), healthcare and public health (14%), and financial services (11%) sectors. Figure 2 shows the distribution of all attacks across critical infrastructure sectors, each of which I discuss in greater detail below.

Figure 2: Terrorist Attacks on Critical Infrastructure in the United States, 1970-2015 (n=2,055)



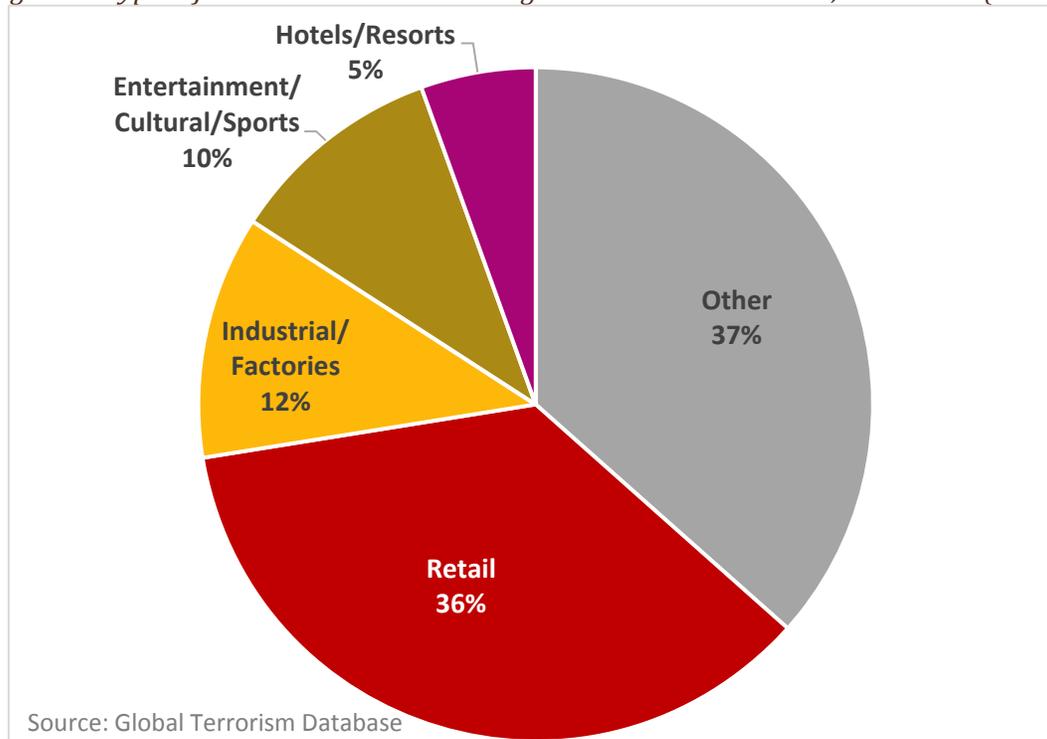
Commercial Facilities Sector

The commercial facilities sector suffered the highest number of attacks between 1970 and 2015, with 454 attacks, causing 39 total deaths. Note that this does not include the implications of the September 11, 2001 attacks on the commercial facilities sector. As noted above, these attacks were classified as having targeted the transportation systems and defense industrial base sectors. Attacks on commercial facilities took place each year between 1970 and 2015, with the sole exception of 2007.

The vast majority (95%) of attacks on commercial facilities were non-lethal, and the deadliest attack took place in 1973, when seven victims and one assailant, a black nationalist, were killed in an attack at a hotel in New Orleans, Louisiana. While most attacks on commercial facilities were non-lethal, more than 1,500 people were wounded in such attacks between 1970 and 2015. These include the 1993 bombing at the World Trade Center in New York City, which injured at least 1,000 people; the 2014 bombings at the Boston Marathon in Massachusetts, which injured more than 260 people; and the 1996 bombing at Centennial Olympic Park in Atlanta, Georgia, which injured more than 100 people. In addition, 89 percent of the terrorist attacks on commercial facilities resulted in some property damage.

As Figure 3 shows, the commercial facilities targeted were nearly all classified as businesses (86%), including most frequently retail stores (36% of all attacks on commercial facilities), industrial facilities or factories (12%), entertainment, cultural or sports venues (10%), and hotels (5%). The remaining targets were very diverse, each comprising less than 5 percent of the total.

Figure 3: Types of Commercial Facilities Targeted in the United States, 1970-2015 (n=454)



The tactics used in these attacks were primarily bombings (55%) and facility/infrastructure attacks (40%), in which the primary objective is to cause damage to non-human targets, excluding the use of explosives. Facility attacks typically involve arson. Less than 3 percent of the attacks on commercial facilities were armed assaults; and kidnappings, barricade incidents, unarmed assaults, assassinations each comprised less than 1 percent of the total.

For nearly one-fifth (19%) of the terrorist attacks on commercial facilities in the United States between 1970 and 2015 no information about the perpetrator(s) was reported in source materials. Among the remaining cases, more than 70 perpetrator organizations and generic designations (e.g., “Cuban Exiles”) were identified, as well as unaffiliated individual perpetrators. The two organizations responsible for the most attacks were the Earth Liberation Front (11%) and the Animal Liberation Front (9%), which were primarily active in the 1990s and 2000s. Two Puerto Rican independence groups active in the 1970s—Fuerzas Armadas de Liberacion Nacional (FALN) and the Armed Revolutionary Independence Movement (MIRA)—followed, with 8 percent and 7 percent, respectively. The remaining attacks were carried out by groups and organizations representing a variety of ideological influences, including left-wing extremists, right-wing extremists, black nationalists, white supremacists, Jewish extremists, environmentalists, and anti-Castro Cuban extremists.

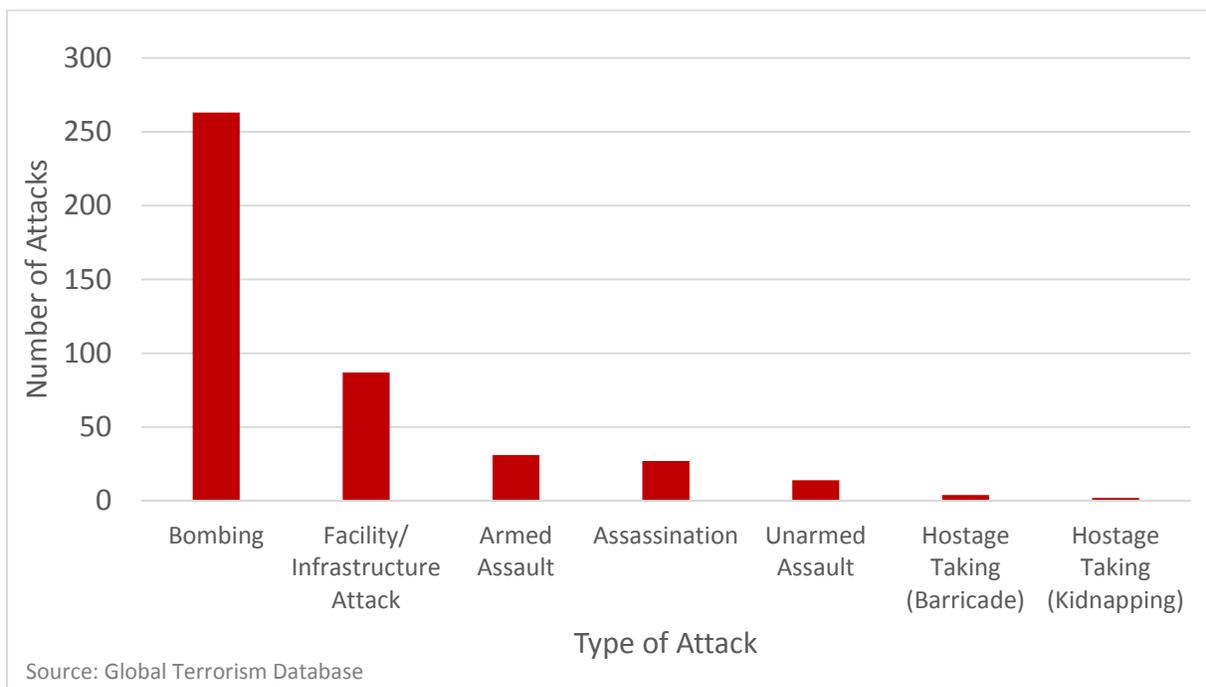
Government Facilities Sector

Terrorist attacks targeting government facilities in the United States also took place nearly every year between 1970 and 2015, with 433 attacks in total. These attacks caused 210 deaths and more than 780 people injured. The majority of these deaths (80%) and injuries (83%) occurred as a result of the 1995 bombing of the Alfred P. Murrah federal building in Oklahoma City. An additional 7 percent of deaths and 3 percent of injuries took place in 2015 when assailants inspired by the Islamic State of Iraq and the Levant (ISIL) carried out an armed assault at a local government facility in San Bernardino, California—the second-deadliest attack against a government facility during this time period. Like terrorist attacks on commercial facilities, 95 percent of all attacks on government facilities were non-lethal.

The most frequently targeted types of government targets were general government buildings and offices (42%), followed by diplomatic targets (e.g., embassies and consulates, diplomatic personnel, and international organizations; 32%). An additional 10 percent of terrorist attacks on government facilities impacted targets associated with the courts system, (e.g., court buildings, judges, and attorneys); 6 percent targeted government personnel; and 4 percent were aimed at politicians and political party targets.

Figure 4 shows the types of terrorist attacks in the United States that targeted government facilities. Compared to terrorist attacks on commercial facilities, attacks on government facilities were somewhat more likely to involve bombings (62% compared to 55%), but half as likely to involve facility/infrastructure attacks (20% compared to 40%). Attacks on the government facilities sector were also much more likely to involve tactics focused particularly on people: armed assaults (7%), assassinations (6%), and unarmed assaults (including the use of chemical and biological agents; 3%). Barricade incidents and kidnappings each comprised less than 1 percent of terrorist attacks targeting the government facilities sector.

Figure 4: Tactics of Terrorist Attacks on Government Facilities in the United States, 1970-2015 (n=433)



For 20 percent of the terrorist attacks on government facilities in the United States between 1970 and 2015, no information about the perpetrator was reported in source materials. The remaining attacks were carried out by operatives of more than 80 perpetrator groups and generic designations, as well as unaffiliated individuals with a variety of ideological influences. These perpetrators of attacks on government facilities were diverse, perhaps even more so than the perpetrators of attacks on commercial facilities. The most common perpetrator designation identified is “left-wing militants,” who were responsible for 14% of the attacks on government facilities, all of which took place in the early 1970s. The second most common perpetrator designation is “Unaffiliated individual(s)” (11%) which refers to assailants who were not known to be associated with a formal organization but were acting in pursuit of one or more ideological goals. This category includes both the 1995 bombing in Oklahoma City and the 2015 assault in San Bernardino. The most prolific formal organization responsible for terrorist attacks on government facilities in the United States was the Jewish Defense League (JDL). The JDL was active in the 1970s and 1980s, and carried out 6 percent of all attacks against government targets.

Healthcare and Public Health Sector

The healthcare and public health sector was targeted in 281 terrorist attacks between 1970 and 2015; however, the pattern of these attacks over time differed significantly from the overall trend. Nearly three-quarters of the attacks targeting healthcare and public health facilities (73%) took place between the mid-1980s and mid-1990s—specifically, 1984 to 1997. Nearly all (97%) of the terrorist attacks targeting the healthcare and public health sector in the United States were non-lethal. Combined, these attacks resulted in a total of 12 deaths and 41 people injured.

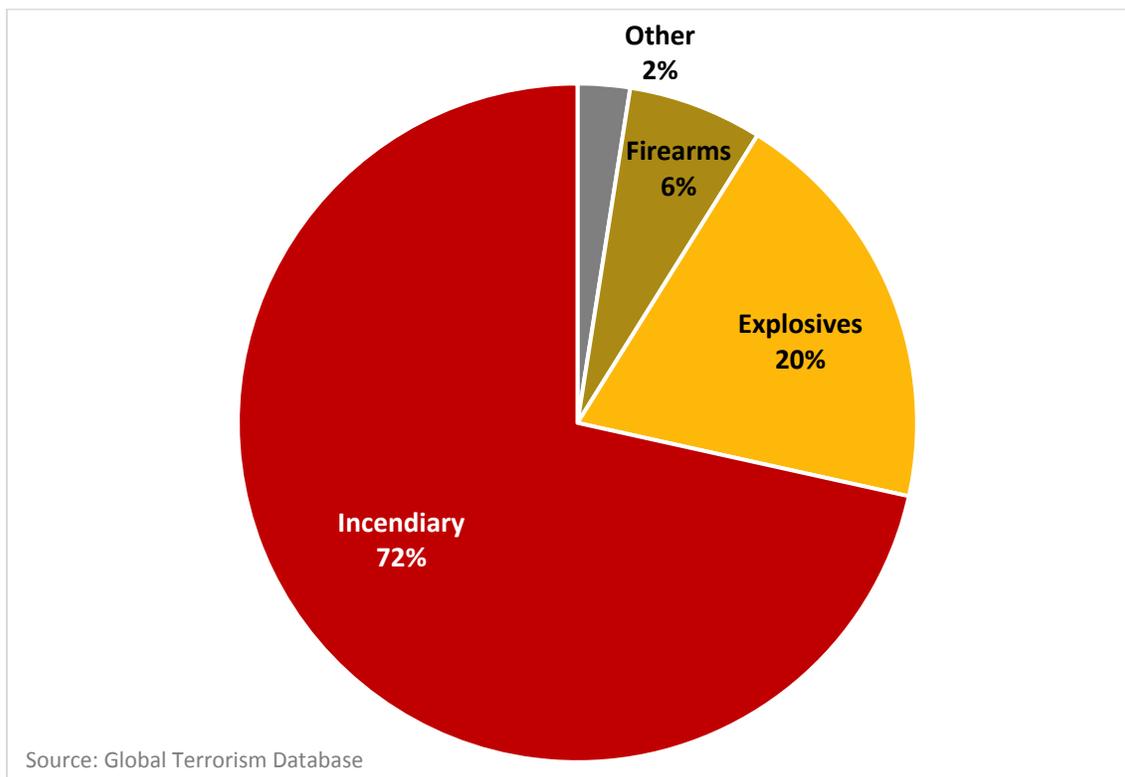
Unlike the other most frequently targeted critical infrastructure sectors (commercial and government facilities), attacks on healthcare were almost exclusively focused on a single type of target—abortion-

related facilities and personnel. Abortion-related targets—primarily clinics—comprised at least 95 percent of all attacks on the healthcare and public health sector in the United States between 1970 and 2015. An additional 4 percent of these attacks targeted clinics and laboratories more generally.

Accordingly, of the cases for which information about perpetrators was reported in source materials (86% of all attacks on the healthcare sector), 88 percent were attributed to generically identified anti-abortion activists or individuals unaffiliated with a particular organization, but nonetheless motivated by anti-abortion ideology. Anti-abortion groups including Army of God (8%), the Christian Liberation Army (1%), and Phineas Priesthood (0.4%) were also identified as perpetrators. Finally, one attack in 1970 was attributed to unspecified revolutionary leftists; one attack in 1971 was attributed to the leftist group Students for a Democratic Society; one attack in 1979 was attributed to the anti-Castro Cuban group Omega-7; and one attack in 2003 was attributed to the Animal Liberation Front (ALF).

Figure 5 illustrates the weapons used in terrorist attacks on the healthcare and public health sector. Nearly two-thirds (72%) of the attacks on healthcare targets in the United States between 1970 and 2015 involved incendiary weapons, including arson materials, gasoline, and alcohol. An additional 20 percent involved explosives, 6 percent involved firearms, and a small number of attacks—2 percent of the total—involved other weapon types such as “melee” weapons (e.g., sharp or blunt objects), vehicles, and biological weapons (specifically, anthrax).

Figure 5: Weapons Used in Terrorist Attacks on Healthcare and Public Health in the United States, 1970-2015 (n=281)



Ten of the 12 people killed in terrorist attacks against healthcare and public health targets in the United States were killed by firearms. This figure includes the deadliest single terrorist attack against a healthcare facility in the United States—the 2015 attack in which an assailant attacked a Planned Parenthood facility in Colorado Springs, Colorado, killing three people. In addition, it includes the first death as a result of a bombing at an abortion clinic—a security guard killed in 1998—as well as one person who died as a result of becoming infected with inhalation anthrax in 2001 at a hospital in New York City. Note that although this last incident took place in the context of a series of attacks involving anthrax in the United States in September and October 2001, the exact circumstances surrounding this particular case are unclear.

Financial Services Sector

The financial services sector in the United States was targeted by terrorists 222 times between 1970 and 2002; however, no terrorist attacks on this sector took place between 2003 and 2015. This does not include the attacks in New York City on September 11, 2001 which, as stated above, were classified as having targeted the Transportation Sector despite having implications for numerous critical infrastructure sectors. Of these, 221 attacks targeted banks or armored trucks, and one involved an attempted bombing at a Diebold office building in Seattle in 1977. Ten people, including one perpetrator, were killed in these attacks.

Table 3: Most Frequent Perpetrators of Terrorist Attacks on the Financial Services Sector, 1970-2002

Perpetrator Group	Attacks	Years Active
Fuerzas Armadas de Liberacion Nacional (FALN)	32	1974 -- 1982
Left-Wing Militants	28	1970 -- 1972
Aryan Republican Army	16	1994 -- 1995
Black Liberation Army	12	1971 -- 1974
United Freedom Front (UFF)	11	1975 -- 1984
Weather Underground	10	1970 -- 1975
Macheteros	9	1981 -- 1998
May 19 Communist Order	8	1976 -- 1981
Chicano Liberation Front	8	1971 -- 1975
Independent Armed Revolutionary Commandos (CRIA)	5	1977 -- 1977
George Jackson Brigade	5	1976 -- 1977

Source: Global Terrorism Database

The majority of the terrorist attacks that targeted financial institutions were bombings (61%), followed by hostage taking (barricade) events (19%), facility/infrastructure attacks (11%), and armed assaults (9%). Table 3 shows the perpetrator groups and organizations that were responsible for the most attacks that targeted the financial services sector. Many of the barricade events and armed assaults involved robberies of banks and armored trucks carried out by organizations in pursuit of an ideological goal, including the Aryan Republican Army, the United Freedom Front, and the May 19 Communist Order. Other groups relied more heavily upon bombings, including the Puerto Rican nationalist group FALN (Fuerzas Armadas de Liberacion Nacional), the Weather Underground, the Chicano Liberation Front, and left-wing militants not known to be affiliated with a particular organization.

Defense Industrial Base Sector

Between 1970 and 2015, 190 terrorist attacks targeted the defense industrial base sector in the United States, resulting in a total of 219 deaths. The deadliest of these attacks took place when al-Qa'ida targeted Department of Defense headquarters at the Pentagon in Arlington, Virginia, on September 11, 2001, killing a total of 189 people and injuring more than 100 others. Thirteen people were killed in 2009 when Maj. Nidal Hasan opened fire on soldiers at Fort Hood in Killeen, Texas. In 2015, five military personnel were killed in one of two armed assaults carried out in Chattanooga, Tennessee by Mohammad Youssuf Abdulazez, who was ultimately shot and killed by authorities. Two attacks in Puerto Rico in the 1970s each killed two Navy personnel, and in seven attacks on defense targets a single victim was killed. Six of these attacks took place between 1970 and 1982, and one occurred at a recruiting facility in Little Rock, Arkansas, in 2009.

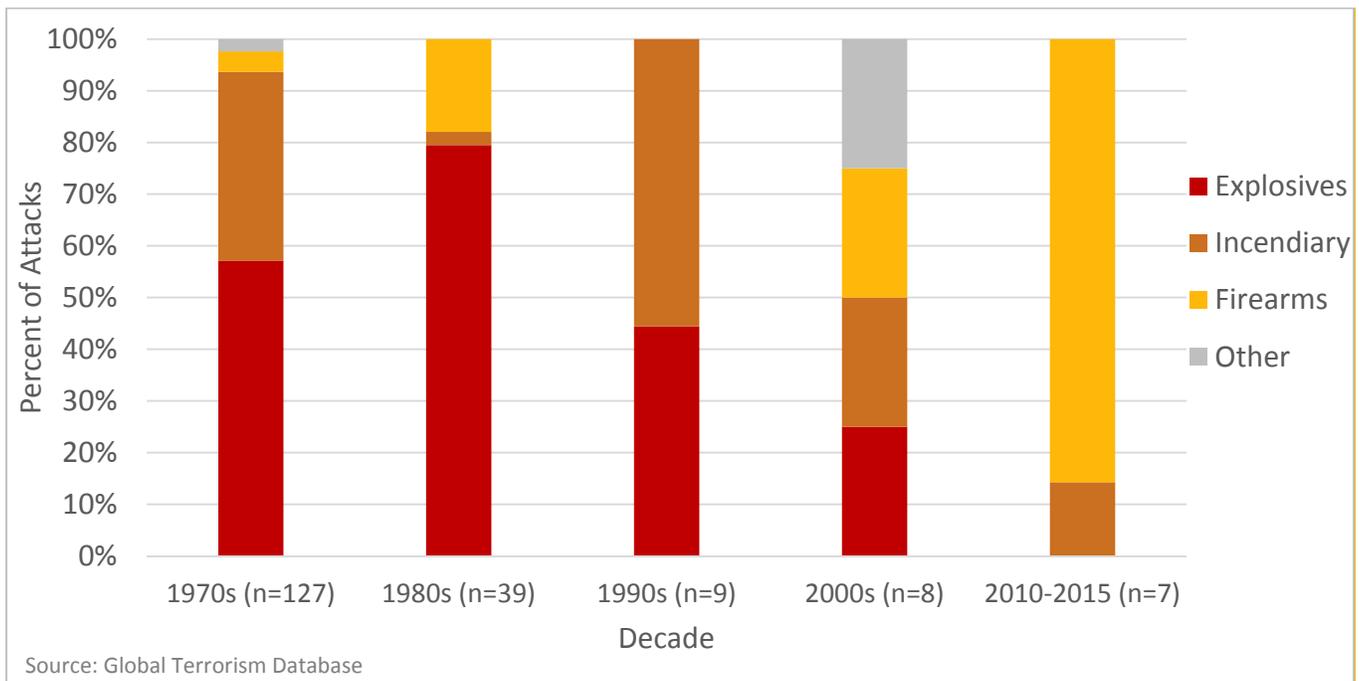
More than half of all attacks that targeted the defense industrial base sector in the United States (52%) took place in 1970 and 1971, when many perpetrators were motivated by opposition to the Vietnam War. The number of attacks against military targets dropped from 67 in 1970 to 32 in 1971 to 3 in 1972 to zero in 1973. During this time period, perpetrators of these attacks were identified as left-wing militants and student radicals. Few attacks were carried out by assailants affiliated with more formally identified organizations such as the Weather Underground.

In the late 1970s and 1980s, perpetrators of attacks targeting the defense industrial base sector were more commonly Puerto Rican nationalist organizations, including FALN, Revolutionary Commandos of the People (CRP), Los Macheteros, and the Organization of Volunteers for the Puerto Rican Revolution. From 1978 to 2001, 73 percent of terrorist attacks against defense industrial base targets (51 attacks) took place in Puerto Rico.

Ten of the 15 attacks in which perpetrators targeted the defense industrial base sector between 2000 and 2015 were carried out by individuals who were not formally affiliated with terrorist organizations. Many of these perpetrators were motivated by radical Islamist ideology and—like the anti-war perpetrators of terrorism the early 1970s—were opposed to United States military intervention in Iraq and Afghanistan, and in one case, Kosovo.

The most common types of targets among terrorist attacks against the defense industrial base sector were military recruiting stations (44%) and military bases or headquarters (34%). An additional 10 percent of attacks on defense targets were against military transportation or patrols. Figure 6 shows the variation over time in weapons used in terrorist attacks against the defense industrial base sector. The progression from the use of primarily explosives and incendiaries in the 1970s, 1980s, 1990s, and 2000s to the use of firearms in the first six years of the 2010s generally reflects shifting patterns of weapon usage in terrorist attacks against all types of targets in the United States.

Figure 6: Weapons Used in Terrorist Attacks on Defense Targets in the United States, by decade (n=190)



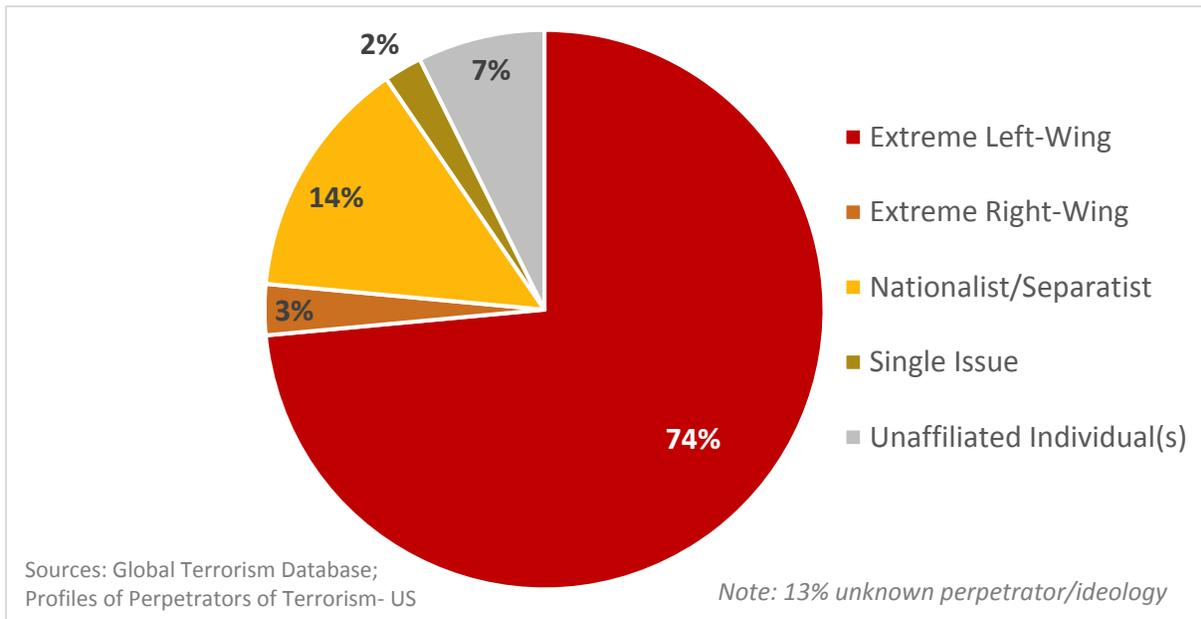
Emergency Services Sector

Between 1970 and 2014, 157 terrorist attacks directly targeted the emergency services sector, killing 57 people. These attacks do not include the attacks of September 11, 2001, which were classified as having targeted the transportation sector and the defense industrial base sector. Nor, does it include other attacks that have impacted the emergency services sector due to its role in security and emergency response. Following an increase in attacks against the emergency services sector, from two attacks that killed two people in 2013 to six attacks that killed 10 people in 2014, there were no terrorist attacks that directly targeted the emergency services sector in 2015.

The vast majority of attacks on the emergency services sector (96%) targeted the police—including both police officers and patrols (60%) and police buildings (36%). In addition, three attacks targeted educational institutions (campus police); two attacks targeted firefighters; and two attacks targeted the personal property of individuals affiliated with policing.

Although there is often overlap in ideological classifications, the perpetrators of attacks targeting the emergency services sector include groups and organizations primarily motivated by extreme left-wing ideology (74%), extreme right-wing ideology (3%), nationalist/separatist ideology (14%), and single-issues (2%), shown in Figure 7. In addition, 7 percent of these attacks were carried out by individuals not affiliated with a particular organization. The ideological motivations of these unaffiliated individuals include anti-government, anti-police, and anti-immigration beliefs, as well as radical Islamist ideology.

Figure 7: Dominant Ideology of Perpetrators of Terrorist Attacks Targeting the Emergency Services Sector in the United States, 1970-2015 (n=157 attacks)



The extreme left-wing organizations that targeted the emergency services sector include the Black Liberation Army, the Weather Underground, and the New World Liberation Front, all of which were active in the 1970s. The extreme right-wing organizations include Posse Comitatus and Aryan Nation, active in the 1980s, a group called Organization 544 that was active in the 1990s, and perpetrators that self-identified with the Sovereign Citizen movement in the 2010s. The nationalist/separatist organizations were primarily Puerto Rican groups active in the 1970s and 1980s, including FALN, Los Macheteros, and the Independent Armed Revolutionary Commandos (CRIA). Single issue organizations that attacked the emergency services sector include an anti-Castro group called the National Integration Front (FIN) and the anti-war People’s Liberation Army (United States), both active in the 1970s, as well as the Earth Liberation Front (ELF), which carried out an attack in the 2000s.

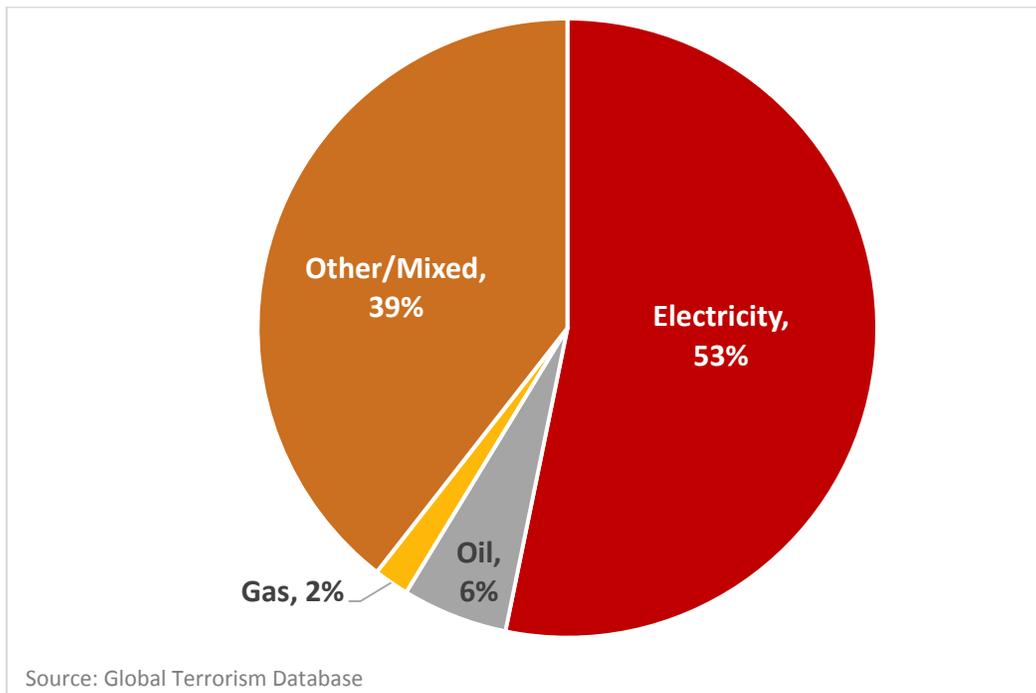
Energy Sector

There were 109 terrorist attacks that targeted the energy sector between 1970 and 2014; none occurred in 2015. Because these attacks were primarily focused on property and infrastructure, they resulted in zero fatalities. Two-thirds of the attacks on the energy sector (70%) took place in the 1970s; 20 percent took place in the 1980s; 5 percent took place in the 1990s; 2 percent took place between 2000 and 2010; and 3 percent took place between 2011 and 2015.

The targets of terrorist attacks on the energy sector included electrical, gas, and oil infrastructure, and in some cases corporate office space belonging to energy companies. Figure 8 illustrates the particular types of targets. Electricity infrastructure and corporations comprised 53 percent of all attacks on energy targets; 6 percent targeted oil infrastructure or oil companies; 2 percent of the attacks targeted gas infrastructure or gas companies; and the remaining 39 percent targeted infrastructure or corporate office

space that was either associated with unspecified or mixed usage (e.g., property belonging to Pacific Gas and Electric (PG&E)).

Figure 8: Types of Energy Facilities/Infrastructure Targeted by Terrorist Attacks in the United States, 1970-2015 (n=109)



These attacks—98 percent of which were bombings (85%) or facility/infrastructure attacks (13%)—were often carried out by unidentified offenders. For one-quarter of all attacks on energy targets, no information about the identity of the perpetrators was identified in source materials. This is consistent with attacks that are more likely to target property and infrastructure. Often the perpetrators were not at the scene at the time of the attack; in some cases they planted an explosive or incendiary device and left. Among the attacks for which perpetrators were identified, more than one-third (34%) were attributed to the New World Liberation Front (NWLF). The NWLF was an extreme left-wing organization that carried out more than 20 bombings targeting the energy sector between 1970 and 1978, primarily aimed at electrical infrastructure belonging to PG&E in California. The remaining attacks were carried out by more than 30 different groups or organizations representing a variety of ideological motivations: extreme left-wing, extreme right-wing, environmentalism, Puerto Rican nationalism, and the anti-Castro movement. Nearly all of the perpetrator groups identified were responsible for one or two attacks against the energy sector rather than a prolonged pattern like that of the NWLF.

Transportation Systems Sector

Between 1970 and 2015 there were 89 terrorist attacks that targeted the transportation systems sector, including the attacks on September 11, 2001. As noted above, although all four of the September 11th attacks targeted aircraft, they impacted a number of other critical infrastructure sectors as well. Three of the attacks—those in which planes crashed in New York and Pennsylvania—have been classified as

attacks against the transportation systems sector, while the one that targeted the Pentagon in Virginia was classified as an attack against the defense industrial base sector.

In addition to these, 10 other attacks targeting the transportation systems sector were lethal. In 1975 perpetrators who were suspected to be Croatian nationalists detonated explosives at a terminal at La Guardia Airport in New York, killing 11 people and wounding 74 others. Two attacks at Los Angeles International Airport (LAX) ticket counters each resulted in three deaths—one involving an explosive device in 1974 and one involving a shooting in 2002. Seven attacks each resulted in one death. The targets of these included a Cuban fishing vessel (1976), Grand Central Terminal in New York City (1976), the Pan American Airlines (Pan Am) terminal at John F. Kennedy International Airport (1981), a Pan Am flight landing in Honolulu, Hawaii (1982), an Amtrak train in Arizona (1995), and most recently two attacks targeting Transportation Security Agency (TSA) agents in 2013 at LAX and 2015 in New Orleans, Louisiana.

Figure 9: Successful and Unsuccessful Attacks that Targeted Transportation Systems in the United States, 1970-2015 (n=89)

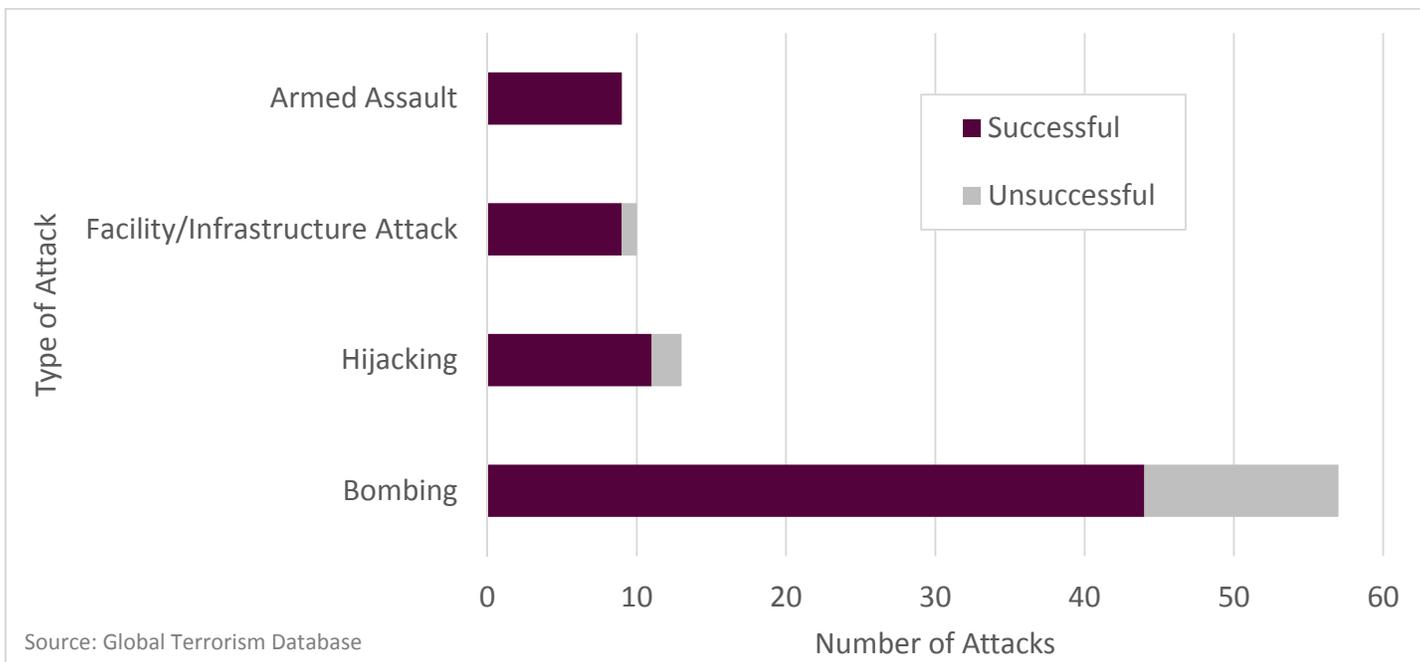


Figure 9 shows the types of tactics that perpetrators used in attacks targeting transportation systems in the United States, divided into successful and unsuccessful attacks. Note that in order to classify the success of attacks we evaluate the extent to which *the intended tactic happened*, once the perpetrator was “out the door” attempting to execute the attack. This definition of success is therefore not a reflection of whether the attackers achieved their ultimate goals, but instead is intrinsically linked to the type of attack. For example, a bombing was successful if the bomb detonated (even if it did not achieve the intended amount of destruction), but unsuccessful if it failed to detonate or was defused harmlessly by authorities. In contrast, a hijacking was successful if the perpetrators successfully gained control of the

vehicle, and an example of an unsuccessful facility/infrastructure attack is one in which the arsonist attempted to but failed to ignite a fire.

Nearly two-thirds (64%) of the attacks on transportation targets were bombings, which had the lowest success rate of all tactics used against this sector (77% successful). The unsuccessful bombing attempt with perhaps the greatest potential lethality is the attempt by Umar Farouk Abdulmutallab to detonate explosives he was wearing on Northwest Airlines Flight 253 upon descent into Detroit, Michigan, in 2009. A similar failed attempt by Richard Reid took place in 2001; however, this particular attack is not included in this analysis because it took place over the Atlantic Ocean.

Hijackings comprised 15 percent of all attacks on transportation targets and involved aircraft in all cases. Prior to the September 11, 2001 attacks the most recent terrorist hijacking in the United States took place in 1984. A total of four terrorism-related aerial hijackings took place in the United States in the 1980s, and six took place in the 1970s, including two unsuccessful attacks in 1970 and 1971.

Ten of the attacks on transportation targets were facility/infrastructure attacks, which are intended to cause property damage rather than loss of life. At least five of these attacks, including one unsuccessful arson attempt, were carried out by animal rights and environmentalist groups. These perpetrators included the Animal Liberation Front (ALF), the Earth Liberation Front (ELF), and a group calling itself the People's Brigade for a Healthy Genetic Future, which set fire to a helicopter being used to spray herbicides on forests in Oregon.

Finally, nine armed assaults targeted people and property associated with the transportation systems sector. All nine of these attacks were successful assaults, meaning that there were either human casualties or property damage caused. Six involved firearms or knives, and three involved incendiary devices of some kind. Specific targets of these attacks included maritime vessels, helicopters, airports and airline personnel/property, and the New York City Subway system.

Food and Agriculture Sector

There were 54 attacks targeting the food and agriculture sector between 1970 and 2015, three of which were lethal and resulted in a total of seven deaths. This includes two attacks in 1975 in which FALN operatives detonated explosives at a restaurant in New York City, killing four people and wounding more than 50, and unidentified perpetrators detonated explosives at a restaurant in San Juan, Puerto Rico, killing two people and wounding 11 others. The third attack—carried out in 1982 and reportedly claimed by the Jewish Defense League—was an arson at a Lebanese restaurant in New York City, which killed one person and wounded eight others. Although non-lethal, two attacks in 1984 in which members of the Rajneeshee religious cult contaminated salad bars in restaurants with salmonella, made more than 750 people ill. The goal of these attacks was to influence local elections.

More than three-quarters of all terrorist attacks on food and agriculture in the United States (76%) targeted restaurants, bars, cafes, or other retail spaces. An additional 16 percent targeted industrial infrastructure, including factories, and 8 percent specifically targeted farms or ranches. Also, most of the

terrorist attacks on food and agriculture (54%) involved incendiary devices or arson. Arson attacks on food and agriculture targets were typically carried out by animal rights and environmentalist groups, including ALF, ELF, and a group that called itself the Farm Animal Revenge Militia (FARM).

Approximately one-third of attacks on food and agriculture involved explosive devices. These attacks took place in the 1970s and 1980s, with the exception of three attacks that took place in the 1990s. The perpetrator groups that most frequently used explosive devices were the extreme left-wing NWLF, the Puerto Rican nationalist group FALN, and white supremacists including members of Aryan Nation.

Three attacks (6%) targeted food and agriculture using firearms. These include two robberies that were carried out by the Black Liberation Army and the May 19 Communist Order, and an additional attack carried out by the Puerto Rican nationalist group called Armed Forces of Popular Resistance (FARP).

The only terrorist attacks on food and agriculture that involved biological weapons were those conducted by Rajneeshees in 1984, described above. And finally, one attack took place in which unidentified perpetrators used chemical weapons—two acid bombs detonated at popular restaurants in Florida in 2010.

Other Sectors

Fewer than 25 terrorist attacks between 1970 and 2015 targeted each of the remaining sectors, including the critical manufacturing sector, the communications sector, the chemical sector, the water and wastewater systems sector, the information technology sector, the nuclear reactors, materials, and waste sector, and the dams sector. Combined, attacks targeting these sectors resulted in two deaths and 11 people injured. In fact, one of the 66 attacks against these sectors was lethal, a 1978 arson attack on a communications facility in San Juan, Puerto Rico.

Conclusions

This analysis of terrorism targeting critical infrastructure in the United States between 1970 and 2015 reveals a variety of patterns and trends. The purpose of this analysis is to demonstrate what types of information are available and provide a general overview of patterns of terrorist attacks against critical infrastructure sectors with respect to patterns over time, targets, tactics, weapons, lethality, and perpetrators, generating additional research themes for future analysis. Possible avenues for future research may include: 1) in-depth analysis of particular attacks or tactics, 2) assessment of attacks that impact multiple critical infrastructure sectors, 3) greater focus on sectors that have been targeted more recently, given that those with greater historical significance may not accurately reflect current tactics/threats; 4) analysis of attacks on critical infrastructure with particular focus on geographic location; 5) consideration of major recent attacks that have targeted critical infrastructure *outside* the United States and potential implications for critical infrastructure in the United States; 6) investigation of the extent to which attacks on critical infrastructure result in property damage; and 7) additional perpetrator-focused research with respect to targeting critical infrastructure, including development of tactical profiles of perpetrator groups as well as greater focus on the role of unaffiliated individuals.