WORKING
PAPER

Rifling Through the Terrorists' Arsenal

Exploring Groups' Weapon Choices and Technology Strategies

BRIAN A. JACKSON AND DAVID R. FRELINGER

WR-533-RC

October 2007

Forthcoming in *Studies in Conflict and Terrorism*

INFRASTRUCTURE, SAFETY, AND ENVIRONMENT

Rifling Through the Terrorists' Arsenal: Exploring Groups' Weapon Choices and Technology Strategies

Brian A. Jackson and David R. Frelinger
RAND Corporation

Forthcoming in ***Studies in Conflict and Terrorism***

Abstract:

In terrorist operations, weapons technologies are the tools groups use to pursue their violent ends. Because of differences in what they can do, different weapons are useful for different types of operations. Using a random sample of terrorist incidents from the RAND-MIPT Terrorism Incident Database, this paper explores (1) how terrorists in general used particular weapons technologies and (2) the variation in the technology choices of individual terrorist groups. The results demonstrate significant differences in the ways different weapons are used, in the versatility of individual technologies, and among the technology strategies of different terrorist organizations.

What sets terrorist organizations apart from other groups with political or other grievances is their willingness to use violence, particularly violence against civilian populations, in an attempt to advance their goals. While the choice to use violence in this way and the targets selected for attack are the key determiners of the overall threat of terrorism and that posed by specific terrorist groups, the weapons and other technologies the groups use to carry out those attacks shape the impact of their operations. For a group, simply desiring to kill or destroy is not enough. It also needs the tools required to make that intent a reality. As a result, understanding the ways terrorist organizations choose technologies and how they use them is a key component of threat assessment and an important input to homeland security and counterterrorism policy design.

Different types of technology can have an impact on terrorist group operations across the full spectrum of activities these groups carry out. Communications technologies and the

Internet have changed the ways such groups exchange information internally and externally.[1] The specific weapons technologies groups choose for attacks define the scale and scope of their violence. The complex infrastructure systems that make much of modern life possible present not just potential targets for attack, but tools terrorist groups might exploit to cause harm.[2]

While all of these technologies and the ways terrorist groups might use them are of interest for developing defensive strategies, much of these groups' technology behavior is difficult to study. Because terrorist groups are clandestine organizations, data on technologies that are used inside groups – and the decisionmaking processes that underlie the choices of what technologies to use and why – are frequently invisible from the outside. What data is available is largely anecdotal which, while useful, cannot provide the basis for more general observations about organizational behavior. As a result, the analyst is left to examine data on uses of technology that are overt and observable almost by definition and are unfortunately much more plentiful – information on the weapons and offensive technologies applied by these groups in attack operations. While not providing the full picture of how these groups interact with technology, analysis of the weapons they use provides a window into group behavior and illuminates one type of technology that is of obvious concern in counterterrorism planning.

In the literature on terrorism, a number of researchers have made observations about groups' weapons choices. Understanding terrorist decisionmaking is a key goal of much terrorism research,[3] and how groups pick weapons and tactics have been explored in larger efforts to assess how terrorists make choices.[4] Detailed examinations have been

---

[1] See, for example, discussion and review in Bruce W. Don, et al., *Network Technologies for Networked Terrorists: Assessing the Value of Information and Communication Technologies to Modern Terrorist Organizations*, TR-454-DHS (Santa Monica, CA: RAND Corporation, 2007).

[2] See, for example, Brian A. Jackson, "Appendix F: Technology and Terrorism," in *The Global Technology Revolution 2020, In-Depth Analyses: Bio/Nano/Materials/Information Trends, Drivers, Barriers, and Social Implications*, edited by Silberglitt, Richard et al., TR-303-NIC (Santa Monica, CA: RAND Corporation, 2006), pp. 209-214.

[3] Reviewed in Gordon H. McCormick, "Terrorist Decision Making," *Annu. Rev. Polit. Sci,* 6 (2003), pp. 473-507.

[4] See, for example, Brian M. Jenkins, "The Terrorist Mindset and Terrorist Decisionmaking: Two Areas of Ignorance," P-6340, (Santa Monica, CA.: RAND Corporation, 1979); C.J.M. Drake, *Terrorists' Target*

done of individual terrorist groups and their technological choices,[5] as well as of single terrorist operations to understand the weapons and tactics that were used to carry them out.[6] Researchers have similarly characterized the range of different weapons terrorists have acquired and the distribution of weapons used across terrorist incidents[7] and made detailed studies of particular weapon types to understand their application in attack operations.[8] These studies of past terrorist behavior provide the basis for one line of argument about terrorist technology preferences: that such groups generally prefer basic technologies – "guns and bombs" – and comparatively simple operations out of a general technological conservatism and desire that their operations be successful.[9]

Selection, (New York, NY: Palgrave MacMillan, 1998); Bruce Hoffman, *Inside Terrorism*, 2nd Ed., (New York, NY: Columbia University Press, 2006); Bruce Hoffman, "Change and Continuity in Terrorism," *Studies in Conflict and Terrorism*, 24(5) (2001), pp. 417-428; and tactical discussion within Gavin Cameron, *Nuclear Terrorism: A Threat Assessment for the 21st Century*, (New York, NY: Palgrave MacMillan, 1999).

[5] For example, Alessia Ceresa, "The Impact of 'New Technology' on the 'Red Brigades' Italian Terrorist Organisation: The Progressive Modernisation of a Terrorist Movement Active in Italy Since the 1970s," *European Journal on Criminal Policy and Research*, 11 (2005), pp. 193-222; Stefan H. Leader and Peter Probst, "The Earth Liberation Front and Environmental Terrorism," *Terrorism and Political Violence*, 15(4) (2003), pp. 37-58; Adam Dolnik and Anjali Bhattacharjee, "Hamas: Suicide Bombings, Rockets, or WMD?" *Terrorism and Political Violence*, 14(3) (2002), pp. 109-128.

[6] For example, James Dingley, "The Bombing of Omagh, 15 August 1998: The Bombers, Their Tactics, Strategy, and Purpose Behind the Incident," *Studies in Conflict and Terrorism*, 24 (2001), pp. 451-465; Andrew Silke, "Beyond Horror: Terrorist Atrocity and the Search for Understanding—The Case of the Shankill Bombing," *Studies in Conflict and Terrorism*, 26 (2003), pp. 37-60; or discussion of the attempted Millenium Bombing by Ahmed Ressam in "The Terrorist Within: The Story Behind One Man's Holy War Against America," online at http://seattletimes.nwsource.com/news/nation-world/terroristwithin/ (as of September 22, 2007).

[7] For example, Richard Clutterbuck, "Trends in Terrorist Weaponry," and G. Davidson Smith, "Sources of Terrorist Weaponry and Major Methods of Obtaining Weapons and Techniques," both in *Technology and Terrorism*, edited by Paul Wilkinson, (London, UK: Frank Cass, 1993), pp. 130-139, 123-129; and Wayman C. Mullins, A Sourcebook on Domestic and International Terrorism: An Analysis of Issues, Organizations, Tactics and Responses, 2nd ed., (Springfield, IL: Charles C. Thomas, Ltd., 1997). Attempts have also been made to correlate choices of weapons with the "success" of terrorist incidents, notably Idris Sharif, *The Success of Political Terrorist Events: An Analysis of Terrorist Tactics and Victim Characteristics 1968 to 1977*, (New York, NY: University Press of America, 1996), though definition of what constitutes success in such efforts and how that definition may have changed over time is problematic.

[8] For example, Chris Quillen, "A Historical Analysis of Mass Casualty Bombers," Studies in Conflict and Terrorism, 25 (2002), pp. 279-292; Dipak K. Gupta and Kusum Mundra, "Suicide Bombing as a Strategic Weapon: An Empirical Investigation of Hamas and Islamic Jihad," Terrorism and Political Violence, 17(4) (2005), pp. 573-598; Marvin B. Schaffer, "The Missile Threat to Civil Aviation," Terrorism and Political Violence, 10(3) (1998), pp. 70-82; and the very recent book by Mike Davis, *Buda's Wagon: A Brief History of the Car Bomb*, (London, UK: Verso, 2007).

[9] Bruce Hoffman, *Inside Terrorism*, 2nd Ed., (New York, NY: Columbia University Press, 2006); Bruce Hoffman, "Change and Continuity in Terrorism," *Studies in Conflict and Terrorism*, 24(5) (2001), pp. 417-428; Rollie Lal and Brian A. Jackson, "Change and Continuity in Terrorism Revisited: Terrorist

The potential effect of new weapons technologies on terrorist behavior has been the specific focus of another body of research with the goal of understanding how technological change might alter terrorist operations.[10] A central component of this literature is broad discussion of terrorist interest in – though limited actual pursuit or use of – unconventional weapons.[11] Efforts to acquire and use such materials would diverge markedly from the view of such groups as technological conservative given the novel and more unpredictable nature of those weapons.

In the history of individual terrorist groups, interest in pursing and using novel technologies has differed from group to group. For example, organizations such as the Provisional Irish Republican Army acquired and used a wide variety of technologies over a long period, while others have focused on one or two attack modes exclusively. Previous studies of how organizations – both terrorist groups and legitimate organizations – acquire and use technology suggest that such differences should not be surprising. The specific characteristics of a group and its environment can significantly influence how it makes decisions regarding technologies.[12] In such studies, the concept of an

---

Tactics, 1980–2005," *Oklahoma City Memorial Institute for the Prevention of Terrorism (MIPT) Terrorism Annual* (2006), pp. 3-18.

[10] For a historical example, see the discussion of how the introduction of time delay fuses changed terrorist activities by enabling campaign type operations discussed in Lindsay Clutterbuck, "The Progenitors of Terrorism: Russian Revolutionaries or Extreme Irish Republicans?" *Terrorism and Political Violence*, 16(1) (2004), pp. 154-181; broader discussions of the effects of new technologies on terrorist operations are included in both Brian M. Jenkins, *High Technology Terrorism and Surrogate War: The Impact of New Technology on Low Level Violence*, P-5339 (Santa Monica, CA: RAND Corporation, 1975); David Ronfeldt and William Sater, *The Mindsets of High-Technology Terrorists: Future Implications from an Historical Analog*, N-1610-SL (Santa Monica, CA: RAND Corporation, 1981) or, a more recent discussion is included in James Bonomo et al., *Stealing the Sword: Limiting Terrorist Use of Advanced Conventional Weapons*, MG-510-DHS (Santa Monica, CA: RAND Corporation, 2007).

[11] This literature was recently reviewed in Nancy Kay Hayden, *Terrifying Landscapes: A Study of Scientific Research Into Understanding Motivations of Non-State Actors to Acquire and/or Use Weapons of Mass Destruction*, (Albuquerque, NM: Sandia National Laboratories, 2007). See also discussion in Bruce Hoffman, *Terrorism and Weapons of Mass Destruction*: *An Analysis of Trends and Motivations*, P-8039 (Santa Monica, CA: RAND Corporation, 1999).

[12] See discussion in Brian A. Jackson, "Technology Acquisition by Terrorist Groups: Threat Assessment Informed by Lessons from Private Sector Technology Adoption," *Studies in Conflict and Terrorism*, 24, (2001), pp. 183-213; Jackson, Brian A., *Aptitude for Destruction, Volume 1: Organizational Learning in Terrorist Groups and Its Implications for Combating Terrorism*, MG-331-NIJ, (Santa Monica, CA.: RAND Corporation, 2005); Jackson, Brian A., et al., *Aptitude for Destruction, Volume 2: Case Studies*

organization's "technology strategy" has been defined to describe how readily it pursues new technologies, the number of different technologies it maintains and uses, and how those technologies are applied in pursuit of its goals.

In examining how organizations use technologies, two related sets of questions are important. The first focuses on the technologies themselves, their characteristics, and their uses. Particular technologies are useful for different things, making them differentially attractive to specific organizations. The second focuses on the nature of organizations and the choices they make regarding which and how many technologies to pursue.

To better characterize the technology strategies of terrorist groups and map the similarities and differences across terrorist organizations, we drew on the data contained in the RAND-MIPT Terrorism Database[13] on the weapons used by terrorist organizations in attack operations. After a coding and analysis effort, the information the dataset contained made it possible to assess:

(1) past terrorist use of weapons technologies to characterize how they have used specific "tools" in the design and execution of their operations.
(2) the weapons choices made by individual terrorist organizations to explore variation in technology strategies across terrorist groups.

The results of such an effort can provide insight into past terrorist behavior and weapons choices, but also are useful for exploring the utility of terrorism incident datasets in technology-focused analyses of terrorist behavior and informing the future design of such datasets to increase their applicability and value.

---

of Organizational Learning in Five Terrorist Groups, MG-332-NIJ, (Santa Monica, CA: RAND Corporation, 2005) and references therein.

[13] The components of the overall *RAND-MIPT Terrorism Database* are the *RAND Terrorism Chronology* (1968–1997) which contains all international terrorism incidents during this period and the *RAND-MIPT Terrorism Incident Database* (1998–present) which contains all terrorism incidents worldwide, including both domestic and international incidents for the more recent period. Varied inclusion criteria for the two data sets mean that there are significant differences in the number and type of terrorist incidents that are included in each. The total number of terrorist incidents per year in the Chronology average in the hundreds, while those in the more recent Incident Database average in the thousands. Much of this difference stems from the broader inclusion criteria (e.g., domestic incidents) used for the Incident Database.

What Do Terrorists Do with Particular Weapons? Assessing How Individual Technologies Have Been Used Across Terrorist Groups

To explore how terrorist organizations have used specific weapons technologies, we began with all terrorist incidents included in the RAND-MIPT Terrorism Database that occurred in the twenty-five year period from 1980 to 2005. This initial dataset contained just over 22,000 terrorist attack operations. Because the focus of this analysis was weapons and tactics, all incidents in which the weapon used in the attack could not be determined from the available descriptive information on the incident were eliminated. From the remainder, a random sample[14] of 5000 incidents was selected for detailed examination and analysis.

Because of the nature of the RAND-MIPT database, which combines a historical database of international terrorist incidents with a contemporary and on-going data collection on both international and domestic terrorism,[15] the contents of the database is biased toward more recent terrorist incidents. Since the historical dataset focused only on international terrorist incidents, many events which would now be included were outside the collection criteria for that effort. As a result, while this discussion draws on information about the way terrorists tactically employed their weapons since 1980, the majority of the data examined focuses on recent events and the contemporary terrorist threat.[16]

---

[14] The sample of incidents was drawn by generating a random sequence containing the numbers from one to the total number of incidents in which a weapon was specified using the SAS statistical package and the PROC PLAN procedure. This random sequence of numbers was aligned with the chronologically sorted listing of the incidents in a Microsoft Excel spreadsheet and the incidents sorted by the random index to randomize their order. The first 5000 incidents in this listing were pulled for analysis.

[15] To the extent that the weapons chosen by terrorist groups for international terrorist operations and domestic terrorist operations differ, these differences in database inclusion criteria represent a source of error in this analysis. These potential differences are likely to be more important for groups that use many different weapons than those which use only a few. The effect of these differences, including the example of the Provisional Irish Republican Army, is discussed in more detail later in the paper.

[16] Of the incidents included in the sample eight percent occurred in the six years between 1980-1985, seven percent in the five years between 1986 and 1990, five percent between 1991 and 1995, eighteen percent between 1996 and 2000, and sixty-one percent between 2001 and 2005.

Weapon Types in the Terrorist Arsenal

Although each entry in the database is coded by weapon type, the legacy categories used in the original database combine some weapon types which we wanted to examine separately. As a result, the first step in our analysis was to examine each incident description in the sample and categorize the incidents *de novo* based on the weapon(s) used in the attack. Each incident was coded as follows:

- Attacks in the database's broad "explosives" category were broken into several separate classes: explosives (to capture bombs and planted explosive devices), hand grenades, rocket propelled grenades (RPG), mortars, and rockets. In addition to breaking out explosives delivered by very different mechanisms, these categories also separate weapons that are usually made internally to terrorist groups (e.g., bombs), from those usually obtained outside the group (e.g., RPGs), and those which might either be manufactured or acquired from external sources (e.g., mortars or rockets.)

- Incidents of manual sabotage – attacks where basic technologies or tools were used to damage buildings, infrastructures or vehicles by hand – were identified (generally from the database's "other" or "unknown" categories) and coded separately.

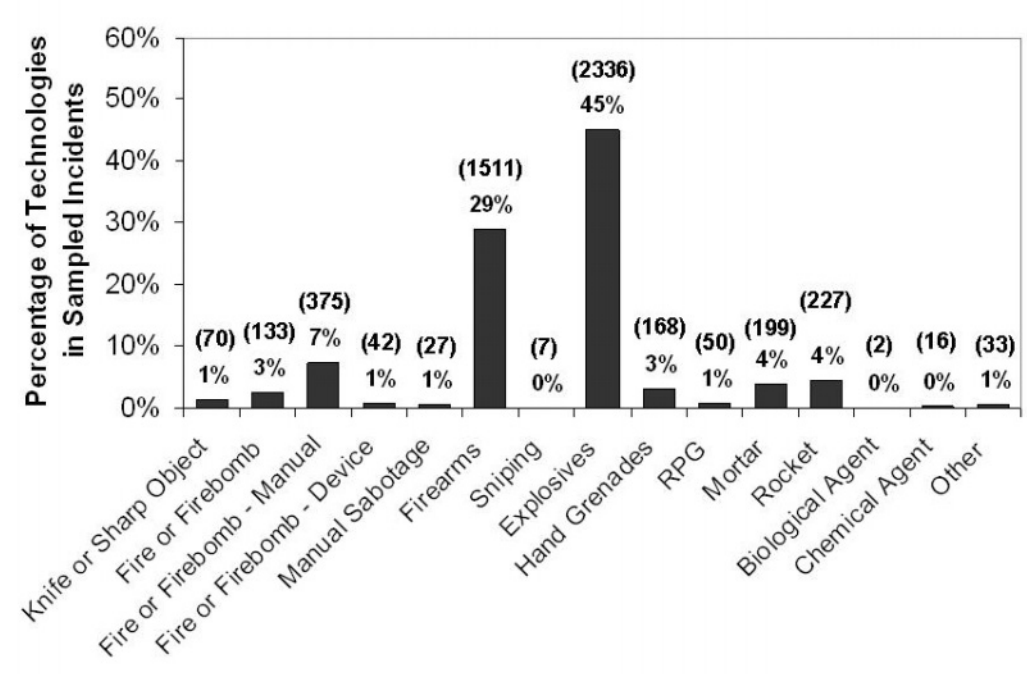
- Incidents involving sniper tactics or equipment were identified and separated out of the database's "firearms" category.

- To the extent possible, the database's "fire or firebombing" category was broken down into simple manual firebombs (e.g., Molotov cocktails) and more complex incendiary devices. This produced three overall categories, "fire or firebomb – manual," "fire or firebomb – device," and the generic "fire or firebomb" category for incidents where a determination could not be made.

- For attacks involving more than one weapon type, all were identified, coded, and linked to the incident.

Looking across the 5000 incident sample, the breakdown of weapons used is presented below in Figure 1.

Figure 1: Distribution of Weapon Types Used in a Sample of Terrorist Operations, 1980-2005



Note: Bars indicate percentage of incidents in the sample (n=5000) which indicated the type of weapon was employed. Counts of weapon uses are included over the bars in parentheses. Total exceeds 5000 due to uses of multiple weapons in single incidents.

More sophisticated explosive-based weapons (notably RPGs, mortars, and rockets) are only a small slice of the overall use of explosives, but nonetheless make up enough of the total weapons used to be worthy of separate consideration. Very few instances of sniping by terrorist groups – a tactic representing the "high end" of firearms use – were present in the sample. Use of unconventional weapons was similarly rare. In a distinct example of comparatively low sophistication weapons dominating terrorist technology choices, of the fire or firebombing incidents which could be categorized, the number of manual "thrown firebombs" outnumbered more sophisticated incendiary devices almost nine to one.

These basic results are consistent with previous results in the literature that explosives and firearms dominate terrorist weapons choices.

Tabulating the Types of Operations Where Particular Weapons are Used

While such overall tabulations of weapons used by terrorist group can provide some insight into the technologies that are attractive to such groups overall, just measuring the popularity of weapons in aggregate only provides part of the picture. Weapons are tools to achieve violent ends, and different tools are useful for different things. Understanding the part specific weapons technologies can play in terrorist groups' activities – and, therefore, their potential attractiveness to different types of groups – requires understanding not just that terrorists used the weapons, but what they used them to accomplish.

To explore the range of tactical applications in which these groups used specific weapons, a typology of terrorist incident types was developed capturing five central classes of operations and a small number of characteristics for each operational type. The goal in developing the taxonomy was to build a set of classes broad enough to capture the range of terrorist behavior, but still simple enough to use, given the limitations in the descriptive data available on each individual terrorist incident. The incident types and the more specific attack characteristics within each type (in italics in the descriptions) are as follows:

1. **Attack on a Specific Individual** – an attack on a specific individual could be intended to either *injure or kill* them (e.g., an assassination) or to *kidnap* them. Depending on the target and the security protecting them, the individual could be coded as *defended* or *undefended*.

2. **Attack on Individuals in General** – an attack targeting people (e.g., individuals in a public space or in a structure) could be intended to *injure or kill* them or to *kidnap* them.

3. **Attack on a Vehicle** – an attack on a vehicle could be intended to either *damage or destroy* it or to *hijack or gain control* of it. Vehicles could either be coded as *defended* (e.g., an armored limousine with a security detail) or *undefended* (e.g., a civilian car).

4. **Attack on a Structure** – like an attack on a vehicle, a strike on a building or structure could be indented to *damage or destroy* it or to *enter or control* it. In some cases, however, terrorist groups have staged operations against structures where the weapons chosen cannot practically accomplish either end – e.g., a single shot fired from a handgun at an embassy. Such operations are viewed as *symbolic* in nature and are coded in a separate category. Structures could be *defended* (e.g., a government building) or *undefended* (e.g., a public restaurant).

5. **Attack on an Area** – In some cases, terrorist actions are aimed not at a point target, but at an entire area. For example, mortar fire into a general residential area or a contaminant introduced into a region's water supply (or a credible threat to do so) would be coded as area attacks. Do to the nature of area attacks, it was generally not possible to ascribe any more detailed intent to individual operations (e.g., whether the attack was intended to injure or kill people or to damage targets in the area).

Using this taxonomy, the available narrative information on each terrorist incident in the sample was reviewed and, to the extent possible, each was coded for its targets, their nature (defended or not), and the apparent intent of the attack (to injure or kill; kidnap; damage or destroy; hijack; enter or control; or to stage a symbolic strike.) The specific decision tree used to code incidents is included in the Appendix. Particular incidents were linked to as many characteristics as appropriate. Not all incidents could be categorized or their characteristics determined.

In some cases, single incidents might have multiple targets and intents. For example, an attack on a political leader's motorcade is aimed at the specific individual riding inside the car, rather than the vehicle itself. In that case, the incident would be coded as an attack on the vehicle (though not intended to damage or hijack it) and as an attack on a specific individual intended to injure, kill or kidnap. In some cases, limits on available information made it impossible to assess what an attack was attempting to accomplish or even what it was targeting. For example, of the 5000 incidents, 100 could not be assigned a likely target either for lack of information or because the incidents described operations that were disrupted before an actual attack was staged.

In considering the results of this coding effort, there are two important caveats that the reader should keep in mind:

- First, it is important to understand from the outset that this research effort is extracting information from a dataset that was not created with this particular application in mind. As is the case with most datasets on terrorist activity, the RAND-MIPT Terrorism Incident Database is dependent on the reporting through media outlets that provide a description of an event and the context within which it occurred. The reporting is by definition non-standardized, and is subject to source filtering by officials controlling disclosure of important information, the writing and editorial process, and in many cases also subject to a translation from another language into English. Consequently, while some information is fairly clear, such as "The attacker used a bomb," it is less clear at times as to what the attacker's objective was since context information such as, "The Mayor was in the building while attending an event," may be omitted from the incident description.

- Second, although some analyses of terrorist behavior can be rigorously quantitative, making assessments of targets and intent is far from an exact science. In some cases, making determinations about the nature of targets and intent of individual operations was straightforward. For example, if a group enters a building and evacuates the occupants before destroying the structure, it is clear

that it intended to damage the building rather than harm the occupants. Clues about intent can be found in the characteristics of the attack – e.g., use of small bombs and fragmentation weapons strongly suggests the targeting of individuals rather than structures. In other cases, making a clear judgment was difficult or even impossible. An attack, which appears in retrospect to be targeting a broad area, could in reality have been an exceedingly poorly aimed targeted strike.

In general, after looking at the outcome of an incident, our assessment often gave the terrorist attack planner "the benefit of the doubt" – e.g., that they were targeting the political leader rather than her limousine, that the incendiary that went off in a store after hours was intended to do so to cause property damage rather than human casualties, and that the mortar or rocket fire landing randomly in a neighborhood was intended to terrorize the entire area rather than simply reflected the incompetence of the group's fire team or their use of lower quality munitions. While the uncertainty inherent in such a process clearly represents a significant complication for analysis, its presence is inherent in any such examination of terrorist group behavior. In the absence of extensive information on a terrorist group's internal deliberations and attack planning, statements about the intent of particular operations will invariably be educated guesses rather than certain statements of fact.

These realities mean that there is a great deal of noise in the data, some of which originates from limits in our coding efforts, but more from the nature of the data on which it is based. As a result, although the output of this effort (summarized in Table 1) represents a consistent effort to assess and code this dataset by one set of researchers, the numbers produced should not be interpreted as quantitatively absolute. To address the inherent uncertainties in such an effort, we have chosen to report the results of our categorization of target characteristics (defended or undefended) and the intent of the operations binned into ordinal ranges to avoid the appearance of false precision that would be created by reporting numerical percentages. Even so, the results are sufficient for more qualitative comparisons of the ways terrorist groups have used individual

weapon technologies in the past and to draw out some broader generalizations and hypotheses about the influence of particular weapon characteristics on terrorist groups' technology strategies.

Table 1 presents the percentages of the incidents using each weapon associated with each of the five attack types. The percentages do not add up one hundred percent because of both rounding and the possibility that a single incident could fall into multiple attack types.

Under each of these broad categories are ordinal indicators reporting what fraction of the incidents fell into that attack type corresponding to each target characteristic (e.g., defended or not) and to each operational intent. Five categories dividing the range from 0 percent up to 100 percent are identified both by number (0 through 5) and shading in the table. In both cases, percentages again may not add to one-hundred percent due to rounding, single incidents having multiple intents, or the absence of sufficient information to identify the nature of the target or the intent of the operation.

The data presented in the table describe how terrorist organizations overall have used weapon technologies. These are clearly not the only ways these weapons could be used. For example, the fact that our sample did not include a case where sniping was used in an attack against a specific, defended individual does not mean that this has not occurred, nor could not occur since sniper operations are clearly useful within this context. However, it does represent a sample of the ways that weapons have been used by these types of groups in the past and a snapshot of the applications for which these groups have found the weapons of use given their unique situations and capabilities. Bearing the necessary caveats in mind, several generalizations can be drawn from this tabulation of weapon types and their applications:

Table 1: Types of Attacks, the Nature of Their Targets, and Their Intent by Weapon

		Knife or Sharp Object	Fire or Fire-Bomb	Manual Sabotage	Firearms	Sniping	Explosives	Hand Grenades	RPG	Mortar	Rocket	Biological Agent	Chemical Agent	Other
Attack on Specific Individual		**29%**	**1%**	**0%**	**37%**	**57%**	**8%**	**11%**	**16%**	**1%**	**4%**	**0%**	**25%**	**15%**
Nature:	Defended	0	2	0	1	0	2	1	1	4	4	0	0	0
	Undefended	4	2	0	4	4	2	4	3	0	1	0	3	4
Intent:	Injure or Kill	4	3	0	4	4	4	4	4	4	4	0	1	4
	Kidnap	2	1	0	1	0	0	1	0	0	0	0	1	0
Attack on Individuals		**66%**	**9%**	**11%**	**51%**	**43%**	**31%**	**62%**	**62%**	**23%**	**16%**	**100%**	**25%**	**64%**
Intent:	Injure or Kill	4	4	4	4	4	4	4	4	4	4	4	2	4
	Kidnap	1	1	0	1	0	1	1	1	0	0	0	1	1
Attack on Vehicle		**7%**	**29%**	**44%**	**28%**	**0%**	**16%**	**14%**	**28%**	**1%**	**5%**	**0%**	**0%**	**12%**
Nature:	Defended	0	1	0	1	0	2	1	3	0	1	0	0	0
	Undefended	4	4	4	3	0	3	4	2	4	3	0	0	4
Intent:	Damage or Destroy	0	4	4	2	0	3	2	4	4	4	0	0	2
	Hijack or Control	3	1	0	1	0	1	1	0	0	0	0	0	2
Attack on Structure		**9%**	**71%**	**52%**	**23%**	**0%**	**63%**	**65%**	**62%**	**28%**	**35%**	**0%**	**63%**	**27%**
Nature:	Defended	0	1	2	2	0	1	1	3	4	3	0	2	1
	Undefended	4	4	3	3	0	4	4	2	1	2	0	2	4
Intent:	Symbolic	0	1	0	1	0	1	1	1	0	0	0	1	0
	Damage or Destroy	0	4	4	2	0	4	2	4	4	4	0	2	4
	Enter or Control	4	1	1	2	0	1	1	1	0	1	0	0	2
Attack on Area		**3%**	**2%**	**4%**	**2%**	**0%**	**6%**	**0%**	**6%**	**70%**	**61%**	**0%**	**6%**	**0%**
Total Incidents Using Weapon		*70*	*550*	*27*	*1511*	*7*	*2336*	*168*	*50*	*199*	*227*	*2*	*16*	*33*

Legend	
0%	0
0% < N ≤ 25%	1
25% < N ≤ 50%	2
50% < N ≤ 75%	3
75% < N ≤ 100%	4

- ***There are significant differences in the types of targets for which different weapons are used.*** Not surprisingly, the use of knives and sharp objects is largely against individuals and, when they are used in attacks on vehicles or buildings it is to gain entry or control. Fire and firebombs are the opposite, being used mainly against structures and vehicles. Firearms and hand grenades are used in attacks across classes, with the exception of area attacks. Explosives are used across all classes, though less in attacks on specific individuals and area attacks than in other types of operations.

- ***There are differences in the weapons chosen for attacks against defended versus undefended targets.*** RPGs, mortars and rockets are largely used for attacks on defended targets – structures and specific individuals for rockets and mortars, and structures and vehicles for RPGs. This can be compared to the use of more general explosives and hand grenades where use against undefended targets dominates. This is not surprising given that the additional investment in these weapon systems (either from sources outside the group or in effort to build them internally) would be less justified if desirable targets could be accessed through other means.

- ***Some weapons enable more flexibility in operational outcomes than others.*** A number of weapons – e.g., mortars and rockets – are rarely or never used in attacks that are not intended to injure or kill or to cause physical damage at the target. As might be expected, such high explosive standoff weapons are unlikely to be compatible with operations with "softer" goals such as hijacking or kidnapping.

The significant differences among weapon types demonstrate that certain weapons are more versatile in the hands of the terrorists than others, and can be used in more ways by these groups. Examining the columns in the table for each weapon type and simply adding up the different ways each weapon was used clearly show that firearms,

explosives, hand grenades, and firebombs have been used in many more ways[17] – against different natures of targets and to achieve more operational goals – than the other weapons. In particular, firearms, explosives and hand grenades stand out for their versatility, given that the use of incendiaries (not surprisingly) is highly concentrated in attacks on structures since people can often avoid the direct impact incendiary attacks. In contrast, others are used in many fewer instances making them more "niche weapons" than broadly applicable tools for terrorist operational design.

Such judgments about weapon versatility can be further illustrated by returning to the narrative descriptions of individual incidents using the weapons. In the sampled incidents, explosives have been used in operational designs ranging from basic bombs in public places up to massive vehicle bombs, but also in bizarre operational designs such as the booby trapping of food items left in public locations. Bombs have been set in ways clearly designed to maximize the casualties produced – and where including multiple devices are used to help assure the operation's success even if some devices fail. At the same time, they have been used in ways where it is clear they were not intended to cause injury or damage at all. In contrast, for other weapons the lack of diversity in use is clear. For example, cases of mortar use are all quite similar, where the weapons are used either to terrorize wide areas or to attack targets that are otherwise protected and inaccessible.

Which Weapons Do Terrorists Use Together in More Complex Operations?

Another factor determining a weapon's versatility is how it can be combined with other weapons in more complex operations. Weapons that are widely useful as "ingredients" in such operations provide attack planners with an even wider range of options and increase their flexibility.

In the sample of incidents examined, one hundred eighty five incidents involved multiple weapon technologies. These were incidents where the description of the attack explicitly

[17] Demonstrated by the very few number of cases where these weapons do not appear in all categories of attacks.

stated that multiple weapons were used (e.g., an attack with both rockets and mortars or an armed assault using both grenades and firearms). Given limits in the information available on many incidents, it is likely that this represents an underestimate of the total number of multi-weapon incidents. For example, if terrorists carried firearms during the planting of a bomb, that incident would meet our criterion of a multiple weapon operation, but the fact that the terrorists did so may not be known or might not be mentioned in the later reports of the incident that provide the basis for inclusion in the database.

Table 2: Counts of Terrorist Incidents Where Specific Weapons Were Used Together

Number of Incidents Where Weapons Are Used Together:	Knife or Sharp Object	Fire or Firebomb	Fire or Firebomb - Manual	Fire or Firebomb - Device	Manual Sabotage	Firearms	Sniping	Explosives	Hand Grenades	RPG	Mortar	Rocket	Biological Agent	Chemical Agent	Other
Knife or Sharp Object						12		1							1
Fire or Firebomb						10		4		1					
Fire or Firebomb - Manual					3	18		4	1			1		2	4
Fire or Firebomb - Device								2							
Manual Sabotage			3			1		1							
Firearms	12	10	18		1			45	22	22	7	5		1	4
Sniping										1					
Explosives	1	4	4	2	1	45			4	1	4	3		1	1
Hand Grenades			1			22		4		1		1			
RPG		1				22	1	1	1		1	1			
Mortar						7		4		1		18			
Rocket			1			5		3	1	1	18				
Biological Agent															
Chemical Agent			2			1		1							
Other	1		4			4		1							

The combinations of weapons in our sample are summarized in Table 2. The uses of multiple weapons are tabulated as pair wise combinations, meaning that a very complex incident where large numbers of weapons were combined (e.g., firearms, hand grenades, and RPGs) will be counted multiple times in the table for each pair of weapons used (e.g., firearms and hand grenades, firearms and RPGs, hand grenades and RPGs.) This was done because the focus of the analysis was the weapon type and the property of interest was how a specific weapon was combined with others in complex incidents.

Across all the weapon types in the sample, every type except biological agents (where only 2 incidents appeared in the sample) was used in combination with at least one other weapon. However, while most weapons could be combined with other technologies in attacks, there were major differences in the extent to which terrorists did so. Table 3 presents both counts of the other weapons with which individual weapons were paired and the percentage of the multi-weapon incidents in which the weapon appeared.

By both criteria, firearms and explosives stand out for their versatility. The weapons were combined with 11 and 12 of the other technologies examined, and appear in approximately 80% and approximately 40% of the multi-weapon attacks respectively. Below these standouts, five other weapons – manual firebombs, hand grenades, RPGs, mortars, and rockets – form a "second tier" for versatility, combined with an average of six other weapons and appearing in an average of 15% of the complex attacks.

Table 3: Versatility of Weapons Technologies Measured by Their Use in Multi-Weapon Attack Operations

Weapon Technology	Number of Other Weapons Paired with in Multiple Technology Operations	Percentage of Multiple Technology Operations in Which Weapon Appears
Knife or Sharp Object	3	8%
Fire or Firebomb	3	8%
Fire or Firebomb – Manual	7	18%
Fire or Firebomb – Device	1	1%
Manual Sabotage	3	3%
Firearms	11	79%
Sniping	1	1%
Explosives	12	39%
Hand Grenades	5	16%
RPG	7	15%
Mortar	4	16%
Rocket	6	16%
Biological Agent	0	0%
Chemical Agent	3	2%
Other	4	5%

What Weapons Do Individual Terrorist Groups Pursue? Assessing Group Technology Strategies

Although terrorist groups may select weapons for reasons unrelated to their operational requirements – e.g., because they believe that possession of a particular weapon will strengthen the image of the group – in general, weapons are tools that are intended to play functional roles. Organizations need technological tools that meet their needs. Because different organizations have different needs, there is no reason to assume that preferences for weapons technologies will be uniform across terrorist groups. Just as the data contained in the RAND-MIPT Terrorist Incident Database can be used to assess how particular weapons were used by terrorists in general, the question can be reversed to examine the weapons choices made by individual terrorist organizations. This provides an approach to catalogue similarities and differences in the way groups choose and use offensive technologies.

For the analyst on the outside and attempting to "look into" a terrorist organization and understand its technology decisionmaking, the ideal situation would be to be able to gather data on the behavior of the group at whatever level individual weapons decisions are made and implemented. For some groups, such choices might be made by a central leadership and imposed on the group as a whole. For others, such choices might be made at the level of individual cells. In such cases, data collected at the group level may obscure differences that might exist among pieces of the larger organization that can be significant in terms of targeting countermeasures against those organizations. Because of the nature of the data available, however, analysts are frequently limited to making assessments at the group level, as attacks are ascribed – or responsibility for them is explicitly claimed – at the level of an entire terrorist group.

To examine the weapons choices of different terrorist organizations, we began with the sample of 5000 terrorist incidents discussed above and sorted the data by the terrorist group responsible. Because of the number of unclaimed and otherwise unassignable incidents, this initial filter eliminated a significant number of incidents from the sample. From the remaining incidents, we selected the top fifty terrorist organizations based on

counts of their attack operations. Because of the scope of the time period covered by the original dataset, the selected groups were not always fully distinct. For example, the set included groups that operated under different names (e.g., Tanzim Qa'idat al-Jihad fi Bilad al-Rafidayn and Tawhid and Jihad) and splinter groups from other organizations (e.g., the Continuity IRA and the Real IRA from the Provisional IRA), all of which are included in the 50 organizations examined.

Since the goal of this analysis was to examine the range of technologies used by individual groups, limiting examination to only the incidents included in the original 5000 incident sample was not sufficient. For the fifty organizations selected, the number of incidents in the data set per group ranged from 141 for Hamas down to only six attacks for several of the groups. The average number of incidents per group was 21. For groups with only a few attacks in the sample, we returned to the original RAND-MIPT dataset and pulled more attacks into this secondary sample for the groups being examined. Additional attacks (also sampled randomly by a procedure analogous to that described previously) were selected to bring the total for the group up to 100 attacks or, for groups where 100 attacks were not available, up to the total number of attacks in the dataset. A full hundred attacks (or greater in the case of Hamas) were only available for 11 of the 50 groups. Attacks per group in the supplemented sample ranged from 141 to 14 and averaged approximately 55 per group (Table 4, second column from the left). The added attacks were recoded and categorized as described previously.

Table 4 presents the distribution of weapon types used by each of the fifty selected terrorist organizations expressed as percentages of the group's attacks in which each weapon was used. The far right column presents the percentage of each group's operations which involved the use of multiple weapon technologies. In addition to reporting the numbers themselves, cells of the table are color coded based on the percentage of particular weapon types to more clearly show how the "spectrum" of technology use varied from group to group. The average distribution of weapons usage across these fifty terrorist organizations (differing somewhat from the distribution in the

original sample of 5000 incidents shown in Figure 1 due to the differences in the sample) is included in the bottom row of the table for comparison.

Even cursory examination of the table demonstrates that very significant differences exist in the weapons choices made by individual terrorist groups. At one extreme of the spectrum lie groups like the Communist Combatant Cells or the Great Eastern Islamic Raiders which used only a single weapon type (explosives) and never combined it with any other weapon. At the other extreme are groups such as Hizballah and al-Fatah which used a majority of the weapons listed either singularly or in multi-technology operations.

It is also the case that many groups deviated significantly from the "average terrorist weapons mix" implied by looking across all the organizations examined. When groups did deviate from that baseline set of technology preferences, the preferred weapons they chose to focus on differed widely. For example:

- Only two groups chose to focus on incendiary devices – the Earth Liberation Front (ELF) and Dev Sol – though drilling deeper into those two groups, the nature of the firebombs they used differed markedly. For Dev Sol, firebombs were simple devices (no cases were categorized as more sophisticated incendiary devices for the group), while ELF used a mix of simple and more complex devices.[18]

- Hamas significantly diverged from average with very large numbers of mortar and rocket attacks, reflecting its need for standoff weapons to address the security barrier around Israel that denied the group the use of suicide operatives.

[18] Preference of ELF for incendiaries, a weapon that requires less expertise on the part of the operative than many other attack modes, is likely also related to the constraints of its exceedingly delocalized structure where individual operatives are largely "on their own" to plan and execute operations. Use of that weapon has fewer learning requirements than many of the others discussed here. See Horacio R. Trujillo, "The Radical Environmentalist Movement," in *Aptitude for Destruction, Volume 2: Case Studies of Learning in Five Terrorist Organizations*, Brian A. Jackson, et al., (Santa Monica, CA: RAND Corporation, 2005), pp. 93-140.

Table 4: Weapons Use Distributions for Fifty Terrorist Organizations, 1980-2005

	Attacks in Sample	Knife or Sharp Object	Fire or Firebomb - Total	Manual Sabotage	Firearms	Sniping	Explosives	Hand Grenades	RPG	Mortar	Rocket	Chemical Agent	Other	Multiple Weapon
Abu Nidal Organization (ANO)	65	2%	3%		48%		37%	18%			8%		2%	15%
Abu Sayyaf Group (ASG)	45	7%			60%		31%	7%	2%					7%
al-Fatah	100	4%			57%	1%	31%	5%	1%	4%	9%		1%	10%
al-Gama'at al-Islamiyya (IG)	36	3%	3%		64%		33%							3%
Amal	59	2%	7%		39%		51%	5%	5%		2%			10%
Ansar al-Sunnah	35	3%			51%		43%		3%	6%				6%
Anti-Castro Cubans	47		4%		11%	2%	85%							2%
Armed Islamic Group (GIA)	48	15%	4%		50%		40%	2%						10%
Armenian Secret Army for the Liberation of Armenia	56		2%		30%		66%	5%						4%
Baloch Liberation Army	24						83%			4%	17%			4%
Basque Fatherland and Freedom (ETA)	100		11%	1%	12%		77%	1%						2%
Black September	15	7%			40%		40%	20%			13%			13%
Communist Combattant Cells (CCC) (Belgium)	15						100%							
Communist Party of Nepal-Maoists (CPN-M)	99	2%	12%		18%		69%						2%	3%
Continuity Irish Republican Army (CIRA)	23		13%		13%		78%			4%				9%
Corsican National Liberation Front (FLNC)	100		1%		9%		91%	1%			2%			4%
Democratic Front for the Liberation of Palestine (DFLP)	22	5%	32%		27%		9%	14%		18%	9%		5%	14%
Dev Sol	41		39%		15%		49%		2%					5%
Earth Liberation Front (ELF)	55		80%	24%										4%
First of October Anti-fascist Resistance Group (GRAPO)	18				6%		94%							
Front for the Liberation of Lebanon from Foreigners	14				14%		86%							
Great Eastern Islamic Raiders Front (IBDA-C)	16						100%							
Hamas (Islamic Resistance Movement)	141	1%			9%		16%	1%		40%	39%		1%	6%
Hizballah	100	3%	4%	1%	24%		58%	4%	1%	2%	8%			5%
Jewish Defense League (JDL)	27		26%		11%		59%					4%		
Kurdish Workers Party (PKK)	48		25%		23%		54%							2%
Liberation Tigers of Tamil Eelam (LTTE)	84	5%			27%	1%	52%	12%	2%	4%				4%
Manuel Rodriguez Patriotic Front (FPMR)	46		22%		9%		72%	4%			4%			11%
National Liberation Army of Colombia (ELN)	100		6%	1%	20%		74%	2%						3%
National Union for the Total Independence of Angola (UNITA)	16				56%		56%				6%			19%
New People's Army (NPA)	52		10%	6%	48%	2%	27%	8%	6%					6%
November 17 Revolutionary Organization (N17RO)	47				15%		57%		4%		23%			
Palestine Islamic Jihad (PIJ)	100	3%			23%		38%	3%		5%	31%			3%
Palestine Liberation Organization (PLO)	27	4%	7%				78%	7%			4%			
People's War Group (PWG)	65	3%	12%	3%	18%		66%						5%	8%
Popular Front for the Liberation of Palestine (PFLP)	54	2%	6%		28%		26%	4%	4%	4%	37%			7%
Provisional Irish Republican Army (PIRA)	51	2%	4%		24%		67%			4%			4%	4%
Real Irish Republican Army (RIRA)	32		9%		3%		78%		3%	3%			3%	
Red Army Faction (RAF)	37		22%		3%		73%		3%					
Revolutionary Armed Forces of Colombia (FARC)	100		3%	1%	29%		62%	2%		3%		1%		1%
Revolutionary Cells	24		13%				88%							
Revolutionary Peoples' Liberation Party-Front (DHKP-C)	22				9%		86%				9%			5%
Revolutionary People's Struggle (ELA)	41		12%				88%							
Shining Path (SL)	100	1%	4%		22%		78%			2%	2%			9%
Taliban	100	1%	9%		46%		18%	2%	3%	1%	24%			4%
Tanzim Qa'idat al-Jihad fi Bilad al-Rafidayn	100		2%		31%		56%		6%	15%	7%			14%
Tawhid and Jihad	25	20%			52%		40%			8%				20%
Tupac Amaru Revolutionary Movement (MRTA)	93		5%		12%		81%	2%	1%		4%			5%
Ulster Defence Association (UDA)	29	3%	14%	7%	24%		52%						3%	3%
United Liberation Front of Assam (ULFA)	62			11%		55%	32%	2%	2%				2%	0%
Average Across Terrorist Groups:	55	2%	9%	1%	23%	0%	58%	3%	1%	3%	5%	0%	0%	5%

Legend
0%
0.1 - 5.0%
5.1 - 15%
15.1 - 35%
35.1 - 60%
60.1 - 100%

- A number of groups used firearms significantly more than average (e.g., al-Gama'at al-Islamiyya, Abu Sayyaf, and al-Fatah).

The differences which exist among groups demonstrate quantitatively that it would be a mistake to assume that all terrorist organizations will adopt similar technology strategies with respect to the weapons they choose.

It is important to note that the nature of the data underlying Table 4 may not fully reflect groups' technology usage, particularly for historical terrorist groups which operated before 2000. Because the data for that time period is drawn from the RAND chronology of *international* terrorism, this produces some artifacts in our analysis. Operations that did not meet the criteria for international attacks[19] were not included in the original database and are therefore not accounted for in this analysis. The case of the Provisional Irish Republican Army is instructive. Although mortar attacks played an important role in its operations in Northern Ireland, those operations did not in general qualify as international terrorist attacks.[20] Mortar operations were used much more rarely in the group's attacks on the British mainland, and therefore the group's overall use of that technology will be underrepresented in the dataset. As a result, the percentage reported in Table 4 for PIRA's use of mortars is likely an understatement. Similar differences likely exist for other groups that carried out a mix of domestic and international attacks over their operational lifetimes before 1997.

---

[19] "Incidents in which terrorists go abroad to strike their targets, select domestic targets associated with a foreign state, or create an international incident by attacking airline passengers, personnel or equipment." (http://www.tkb.org)

[20] See discussion of PIRA in the relevant sections of both Jackson, Brian A., et al., *Aptitude for Destruction, Volume 2: Case Studies of Organizational Learning in Five Terrorist Groups*, and Jackson, Brian A., et al., *Breaching the Fortress Wall: Understanding Terrorist Efforts to Overcome Defensive Technologies*, MG-481-DHS, (Santa Monica, CA: RAND Corporation, 2007) for further discussion of the group's use of mortars.

What are the Implications of Different Groups' Technology Choices?

While the fact that different terrorist organizations choose to use different distributions of weapons is interesting and a relevant input to threat analysis, is there more to these observations than simply that groups can differ in this respect? Though incident data alone are not enough to fully characterize the consequences of different groups' weapons choices, the implications of different technology decisions do go beyond just what types of attacks should be expected from particular groups. To provide the basis for discussing the potential implications of the differences, it is useful to consider how these groups learn and adapt to new operational situations and the components that contribute to groups being successful in carrying out attacks.[21]

Whether a terrorist operation can be executed successfully depends on a number of factors: whether the group has selected an appropriately vulnerable target, whether the group has weapons that are effective against it, and whether the operatives involved have sufficient expertise. Groups that can bring together the right ingredients will be more likely to be successful. To improve their chances, groups can attempt to learn and improve in all of these areas: in casing targets to better determine their vulnerabilities, by obtaining more effective weapons or ones better matched to the types of targets they want to attack, or by improving their own skills.

With respect to weapons technologies, a group's chances of success in a given operation will be shaped by whether it has an appropriate weapon available to strike the chosen target. An organization could develop or acquire new weapons for every operation, thereby ensuring the best match between their requirements and weapon capabilities, but doing so would be slow and would limit the number of attacks it could carry out over time.

---

[21] Jackson, *Aptitude for Destruction, Volume 1: Organizational Learning in Terrorist Groups and Its Implications for Combating Terrorism*; Jackson, et al., *Aptitude for Destruction, Volume 2: Case Studies of Organizational Learning in Five Terrorist Groups*.

The data on groups' weapons choices suggest two different technology strategies groups have adopted to address this problem. The first is to have many tools available in the group (a "***variety***" technology strategy), thereby increasing the chance that – when the organization identifies an attack opportunity – it will already have a tool "on the shelf" that is appropriate to the task. In Table 4, the average number of weapons technologies used by groups is five. Twenty of the fifty groups used more than five different weapons, and five used more than seven.

A variety strategy is not without costs. Previous studies of how organizations build and maintain technological and other capabilities have demonstrated that maintaining skills in many different things takes an ongoing investment of time and effort. If a group doesn't use a technology for an extended period and does not make the investments in practice or training to keep the capability, it will be lost. As a result, a variety strategy will be easiest for organizations that have more human and other resources and run many operations, thereby maintaining skill in its attack modes through repeated use.

An alternative to maintaining many technology options is to focus on weapons that can be used many different ways for a wide range of attack types. Such a "***versatility***" technology strategy reduces the burden on the group (since it only has to maintain its skills in a few weapons, rather than many) but may mean that the weapons it has available are not as well matched to all attack opportunities. Looking at the groups in our sample which chose to use three or fewer weapon types, almost all used either firearms, explosives, or both (the most versatile weapons in the sample, as described above) at rates greatly exceeding the average. The two exceptions to this are ELF, which concentrated almost entirely on incendiaries, and the Kurdish Workers Party (PKK), which used explosives and firearms at near average rates but otherwise focused on incendiaries.

Some weapons are inherently versatile – firearms, for example, are a technology that terrorist organizations can use for many things simply because of the range of operational designs in which they can play a part (see Table 1). To use a firearm in a kidnapping

versus an assassination, it is unlikely the terrorist will have to make any modifications to the weapon itself.

In contrast, for groups to realize the full versatility of other weapons they must know enough about them to be able to modify and customize them to their needs. Explosives are a good example – while the data show that terrorist groups have used explosives for many purposes, aggregate numbers hide great diversity in the ways the weapon has been applied. Bombs cover a range from simple thrown weapons to devices that are detonated through a wide range of means, whether through timers, remote control, or other initiation mechanisms. While some groups obtain their technologies from outside and, as a result, may not be able to customize them for their own needs, other terrorist organizations build up the knowledge and expertise to develop and make these technologies for themselves. In that case – a distinct technology strategy that might be called "***specialization***" – the group can directly shape the weapon itself to match the needs of a particular operation.

Specialization and customization strategies can be used to increase the versatility and performance of weapons that are not inherently flexible. A good example is PIRA's use of mortars, where the fact that the group engineered and manufactured the weapons themselves allowed them to customize their systems to be used in many more ways that are supported by "commercial" systems, including triggering them with timers, engineering up the size of the charges used for increasingly hardened targets, and using the weapons in horizontal modes as direct rather than indirect fire weapons. The flexibility associated with specialization strategies can also let groups modify the performance of their weapons, enabling them more control over the outcome of operations. A simple example of such behavior is rigging weapons so they do not actually detonate – for demonstrative but non-lethal attacks.

Conclusions

While reflecting only a part of terrorist groups' use of technology, examination of the weapons these organizations choose to use in attacks can provide a window into their choices and decisionmaking. Those choices are driven in part by the nature of available technologies, which we explored through a basic analysis of the range of ways terrorist groups had used particular weapons, the characteristics of the targets they struck, and the apparent intended outcome of the operations. The results of that analysis provide a first order measure of the versatility of different technologies based on their range of use and whether they could be readily paired with other technologies in complex operations.

The characteristics we examined are clearly not the only factors which likely shape decisionmaking within terrorist groups. There are important differences among weapons that go well beyond their basic capabilities and their appropriateness for defended versus soft targets. Some weapons give the terrorist organization the option of trading of human resources for technical systems that can be left unattended at targets, some are easier to use in parallel to help ensure operational success, some enable attacks from extended stand-off distances, and so on. As a result, while our analysis has demonstrated differences in the way technologies have been used, we have not explored all the differences that are likely important in shaping terrorists' weapons decisionmaking.

Looking at individual terrorist organizations, we have also shown significant differences in the weapons they have chosen – both in the number of weapons used by each group and the spread of weapons across the full spectrum of possible technologies. Although there is a clear preference for guns and bombs in many groups, what technologies groups choose to use outside of those fundamentally versatile weapons varies considerably.

In assessing individual groups' technology strategies, a terrorist organization's ability to take advantage of opportunities to stage attacks will depend on whether it has, or can get, the tools needed to do so. For groups that maintain expertise in a *variety* of technologies, the chance they will have the "right tool available" as new opportunities arise increases.

For those that do not, focusing on *versatile* technologies may mean they have a tool that is "good enough" to capitalize on an opportunity – and the groups which did limit themselves to a few weapons do indeed appear to focus on the versatile ones. For those technologies where it is appropriate, and for groups that can, *specialization* to enable customizing weapons to attack opportunities can help to better meet operational needs, though it requires the group invest in the capability and expertise needed to do so. Such technology strategies, as lenses through which to view group's weapons preferences and available options, can provide an additional tool for analysts' seeking to understand and anticipate how groups may – or may not – be positioned to respond to new opportunities or changes in their environment.

While quantitative data on past weapons choices will never be sufficient to fully understand the decisionmaking process behind them, bringing together the two halves of this analysis – on the ways weapons have been used by terrorists in general and the specific weapons choices of particular groups – with broader insights on how groups plan operations and adapt to their circumstances is instructive. The results of this analysis also suggest ways that future information gathering focused on terrorist operations and behavior could be improved. Our ability to ask detailed questions about terrorist technology use and what groups sought to accomplish when they used specific technologies was hampered by the fact that current databases are not designed to capture all the relevant data necessary to do so. Though we sought to make our coding of the intent of specific attacks as transparent as possible (e.g., through inclusion of the specific taxonomy in the Appendix to this paper), the results of that coding process necessarily required some judgments. To the extent that using terrorism incident data to assess group technology behavior is useful, additional information could be collected and included in incident databases to make identifying the intent of particular operations more straightforward. For example, broader contextual information may be reported about a terrorist attack that would make its intended outcome more clear but might not be recorded in a database where the primary goal is to capture a more limited set of facts about each incident. The enhanced data might simply be in the form of link to the original source material, or could include excerpts from the original material that would

have a high probability of providing contextual information for later researchers. Furthermore, in populating incident datasets, systematic methods similar to the coding taxonomy described in this paper could be used to include the apparent intent of individual operations as a database field – making it much easier to recognize shifts in the way terrorist groups are using particular weapons or tactics over time.

Appendix: Complete Incident Coding Scheme

The basis of the analysis described in the paper was the coding of a sample of terrorist incidents based on the specific weapon (or weapons) used, the target of the attack, and the apparent intended outcome of the operation. Coding of weapon type was based on the mention of the weapon in the incident description as described in the text. Coding of the targets of the attack were scored as follows:

- Attacks were coded as *attacks on a specific individual* if the incident description mentioned a specific person (Ambassador Smith, "the district chief," the Interior minister, John Doe who was a suspected informer) or that the attack was on someone from a small category of people where the attackers seemed to have singled out the person as members of that category for attack (e.g., two journalists were kidnapped, but not "two Sunnis"). Individual members of the military, government officials, and members of law enforcement organizations on duty were scored as *defended* (as they were likely to be armed or protected by a security detail) and all others were scored as *undefended*.

- Attacks were placed into the more general category *attacks on individuals* when they targeted members of the general public or members of a large subset of the general population. Such individuals were considered undefended by definition, so no categorization based on that criterion was made.

- An attack was coded as an *attack on a vehicle* if the incident description mentioned a vehicle. Military, government, and law enforcement vehicles likely

to be armored, have associated security, or armed occupants were coded as *defended*. All others were coded as *undefended*.

- An attack was coded as an *attack on a structure* if it occurred in or on a building. Government buildings, military installations, law enforcement stations, Israeli settlements, and any site where armed guards were mentioned in the incident description were coded as *defended*. All others were coded as *undefended*.

- An attack was coded as an *area attack* if it appeared to be an indiscriminate attack on a wide area (e.g., mortar or rocket fire into a general area, contamination of a water system, many bombs planted in a variety of public places in a city at the same time, etc.) rather than targeted as specific locations.

Just as individual incidents could utilize multiple weapons, they could also be coded as involving multiple targets. For example:

- An attack could be both an attack on a specific individual and an "attack on individuals" (e.g., a large scale bombing of a parade that killed a political official and many others would be both since both killing the specific person and the members of the general public was inherent in the design.)

- An attack on individuals could also be an attack on a structure (e.g., a large bombing of a building with people in it would be both an attack on the building and the people.)

- An attack on individuals could also be an attack on a vehicle (e.g., a hijacking of an occupied airliner would be both an attack on a vehicle, and also the individuals in it.)

The coding of intent was much more difficult than categorizing the targets of incidents. While the information on the targets of attack is generally clear in incident descriptions,

truly discerning intent would require knowing what the terrorist were thinking at the time the incidents were staged. This scoring is therefore the most uncertain element of the analysis. The intent of specific terrorist incidents was scored as follows:

- If the attack resulted in the kidnapping of the individual (for both incidents targeting specific individuals or individuals more generally), then it was a *kidnap*. If the incident did not mention kidnapping and weapons with the potential to injure or kill were discharged or used in the operation, then it was coded as intending to *injure or kill*. When someone was abducted and subsequently killed, it was coded as both.

- For attacks on vehicles, there were two possible intents – to *damage or destroy* the vehicle and to *hijack or control* it. However, even if a vehicle was targeted in an attack, the incident was not forced into one of these categories. For many operations, the fact that the attack was on a vehicle could be incidental to the actual goal of the attack. For example, if a terrorist group attacks a VIP's motorcade, it would be misleading to suggest that the intent of the attack was to damage the individual's limousine – rather than (or even in addition to) kidnapping, injuring, or killing the occupants.

  Identifying if the intent of the attack was hijacking was usually straightforward from the incident description. Making the distinction between attacks where the involvement of a vehicle was incidental versus those actually targeting the vehicle was scored as follows:

  - With two exceptions (described below), if there were people in a vehicle when it was attacked who could be injured or killed by the operation, then it was assumed the people were the target, not the vehicle. These incidents were therefore not scored as having an intent associated with the vehicle.

- Damaging or destroying the vehicle was inferred as a goal of the operation when:

    - The attack was on an empty vehicle (there is admittedly some uncertainty in this categorization: a bomb which detonated in an empty vehicle could have actually been targeting its occupants but went off prematurely.)

    - The nature of the attack was such that the injuries to the inhabitants could only happen as a result of damage on the vehicle rather than the use of the weapon (e.g., sabotage to train tracks leading to derailment that then hurt people). It was then coded both as seeking to damage the vehicle and harm the passengers.

    - The attack was on a military or security forces vehicle or supply convoy truck (i.e., given the nature of the vehicle and the terrorist conflict, the vehicle itself could be considered a symbolic target or the group had something to gain by the destruction of the vehicle itself or the materiel it carried, not just the people in it (e.g, an attack on a military supply convoy in Iraq.))

- For attacks on structures, there could be three associated intents: symbolic, damage/destroy, or enter/control.

    - An attack was symbolic if it was nominally an attack to damage the building, but its impact could not practically be significant – e.g., a single gunshot fired at the outside of an embassy from a moving car. If a single explosive or firebomb was thrown by hand at the building from outside, the attack was also coded as symbolic since the chance of such an attack significantly damaging the structure itself was very small.

- If the attackers entered the structure and took control of all or part of the building for any period (e.g., an embassy takeover or forcibly entering through a security perimeter to stage an internal attack) then it was coded as enter/control.

- Where it appeared that damaging the structure itself was a central goal of the attack (e.g., bombing or incendiary attack on infrastructure, commercial, or political buildings), then it was coded as damage/destroy.

- Like vehicles, an attack on people inside a building where the building itself appeared incidental were not associated with any of these three intent choices (e.g., a suicide bomber blowing himself up or the use of a primarily fragmentation weapon in a restaurant was coded as aimed at the people rather than the physical structure of the restaurant). However, if the attack used weapons where it was clear the structure would be significantly damaged in the operation (e.g., not just a fragmentation bomb aimed at the people inside it as mentioned above but a significant blast device) then it was coded as intended to damage or destroy the structure as well as harm the occupants.