Technology Acquisition by Terrorist Groups: Threat Assessment Informed by Lessons from Private Sector Technology Adoption[1]

Brian A. Jackson
Center for International Science and Technology Policy
Elliott School of International Affairs
George Washington University

and

The RAND Corporation
Science and Technology Policy Institute

ABSTRACT:

Because of the importance of technology to the operations of modern terrorist organizations, the factors which affect the technological sophistication of extreme organizations are of great interest. In this paper, the process through which terrorist groups seek out and deploy new technology is examined by bringing to bear the deep literature which exists on technology adoption by commercial organizations. A framework is described which delineates not only the factors that influence a group's decision-making processes surrounding new technology but also the obstacles which stand in the way of the successful absorption and use of unfamiliar technologies by a terrorist organization. This framework, by taking a holistic view of the entire technology adoption process, sets out a methodology to both more reasonably predict the outcome of a group's technology seeking efforts and to speculate about its future innovation efforts. Such a technology-focused viewpoint provides a route to more fully inform risk assessment especially with regard to the low probability-high consequence technologies which have served as the focus of much recent counter-terrorist deliberation. The lessons provided by the framework with respect to weapons of mass destruction terrorism and to novel counter-terrorist routes are discussed.

TECHNOLOGY AND TERRORIST ORGANIZATIONS:

Terrorism, the systematic and premeditated use or threatened use of violence for politically motivated purposes, has been called the "weapon of the weak." By staging attacks which are unexpected and which intimidate a larger audience than their immediate victims, a small group of terrorists can influence public opinion and, through this, gain a measure of control over the policies of much larger and militarily stronger nations. Although there was a period in history when hidden daggers and public murder were sufficient to generate such fear, today, terrorist campaigns are far larger in scope and innovative in their methods. Like all modern warfare, advances in military technology have greatly broadened the operational possibilities of today's terrorist groups and have made possible significant increases in their scale. It is the technology which is applied by the terrorist – the explosive device which destroys a target, the automatic weapon which intimidates and, potentially, the chemical or biological weapon which inflicts mass casualties – that make today's "high impact" terrorist strikes possible and makes the threat of future violence credible to a mass audience.

In addition to the role of military technology in terrorism, it is also important to appreciate the broader effect of technology on the potential activities of terrorists. It is a trite but relevant observation that technology has affected almost every part of modern human existence. Transportation systems make it possible to traverse the globe in remarkably short periods of time, trade and product distribution systems deliver perishable goods thousands of miles to their eventual consumers, power generation and water networks make energy and clean drinking water as accessible as flipping a switch or turning on a tap, and, most recently, the linkages of millions of computers into the Internet has made an international information distribution system accessible to anyone who can type. These advances in technology and, more specifically, the interconnectedness and interdependencies they entail have also made modern society increasingly more vulnerable to terrorism. For every advance that improves the quality of life there is a corresponding new vulnerability: airliners can be blown up, a poisoned consumer product can be efficiently distributed to many potential targets, electrical substations can be destroyed plunging cities into darkness, and sites on the Internet are vulnerable to tampering or direct cyber-assault.

Although technology is key to the credibility and effectiveness of a terrorist threat, it is also the main driver behind improvements in counter-terrorism. In response to the threat of hidden weaponry, detection devices such as metal detectors and x-ray machines have been deployed at vulnerable and attractive targets. Given the potential for use of chemical and biological weapons, one goal of current counter-terrorism research is developing methods to detect and defeat these new categories of threats. Beyond detection technologies, the abilities of modern computer systems to collect information, process data to identify patterns, and allow investigations by law enforcement in disparate countries to benefit from each others' work have also been of utmost importance in fighting terrorist groups. This relationship between the technology of terrorism and the technology of those fighting it can be viewed as one of the more important modern arms races, not between superpowers in missile construction but between small groups and states vying for the ability to either perpetrate or prevent low intensity conflict.

The centrality of technology to all terrorist and counter-terrorist operations represents an important incentive for individual groups to seek out and master new techniques and weapons. Although the desire for new technology by terrorist groups is not new – Karl Heinzen discussed the necessity of new technology for terrorist groups as early as 1849[2] – it has been reinforced as society-as-a-whole has become more advanced. The competition between terrorist and anti-terrorist technologies, called by Bruce Hoffman "the technological treadmill,"[3] is a direct selective pressure on terrorist groups – those that cannot remain a step ahead will be overtaken and captured. Furthermore, the opportunities presented by the technological dependence of society will also be inaccessible unless terrorist groups master the techniques necessary to capitalize on them. Although the Internet can make it possible to attack enemies, gain intelligence, accumulate financial resources, and publicize the agenda of a group, in the absence of computer skills, many of these options are inaccessible.

For groups seeking legitimacy and "respect" in today's technologically advanced world, the sophistication of a group's attacks can be of utmost importance. Such a distinction is important both for public reactions – where a more technological attack may result in greater impact[4] – and in the ability of the terrorist to gain the attention of the world press necessary to transmit their propaganda to a broad audience. This pressure to gain media attention and

prominence has been suggested as one of the reasons why terrorist acts in recent years have gradually escalated in their scale and lethality.[5,6] New technologies and weapons are absolutely necessary in the escalation and, as a result, the ability of a group to absorb and deploy them is a critical factor in determining the success of this escalation process. If, for example, a group familiar with simple hand thrown explosives was unable to master sophisticated timing and detonator technology, delayed action and remotely detonated devices would be inaccessible and the group's effectiveness and ability to escalate their operations would be constrained. Taking this point to a more general level, groups which are unable to take advantage of opportunities made available by new technologies, risk being displaced from the world stage and surpassed by competitor groups which can.

Given the broad appreciation of the importance of technology in terrorism, the technical sophistication of terrorist groups and their capability to stage complex operations have long been an element of terrorist threat assessment. Studies of the topic have included consideration of the causes and consequences of terrorist weapons choice, how technological advance has shifted the 'balance of power' between terrorist and counter-terrorist forces, the technological requirements for counter-terrorism, and the terrorist threat of weapons of mass destruction (WMD, including nuclear, radiological, chemical and biological weapons.)[7,8,9] Most studies of terrorist groups and technology, at least those available in the open literature, have approached the topic from a static frame of reference. The focus of examination has generally been the *effects* which advances in technology have had on terrorists' operational possibilities and the potential consequences for society rather than the *process* through which technology adoption occurs.[10] Often, technological acquisition by groups is assumed to be relatively straightforward – through purchase of new weapons or ready access to recipes for chemical or biological agents, for example – and to occur rapidly. Such a view is understandable, given that it is the consequences of terrorists' technological advancement which gain national attention in front page news pictures and television special reports.

Work in the broader field of technology studies, however, has shown that the process of technology acquisition by *any* organization is often a very complex process which is both promoted and inhibited by many different pressures and variables. Such studies have sought to explain, for example, why different companies with access to the same technologies might use

them at varying levels of effectiveness, why the possession of a "recipe" for an industrial process is often not sufficient to successfully replicate it, and why even conscientious attempts to transfer knowledge or technology between different organizations can and do fail. In light of this deeper understanding, it is relevant to re-examine the topic of technology and terrorism from a dynamic perspective by examining not what happens when terrorists gain a new technology but the steps and missteps which are taken as part of the acquisition process.[11] Understanding this dynamic is of particular relevance for contemporary problems in technology and terrorism – including terrorist use of weapons of mass destruction and the Internet as a terrorist tool or venue for attack – and could suggest novel routes to discourage or inhibit the adoption and deployment of new technologies by such groups.

Since terrorist organizations do not generally open themselves to direct study, an understanding of their technology acquisition processes must be approached indirectly. In this attempt, it is profitable to draw on the deep literature on how technology is acquired and applied by *commercial* organizations. Like most studies of clandestine groups, such an inferential approach provides a way to bring together available data and highlight the transferable insights that emerge. From the viewpoint of such a literature, the terrorist organization is simply a "business" which, rather than producing financial profits, endeavors to produce fear and media coverage – the "coin of the realm"[12] in terrorist circles – which are spent to pressure governments or the public to further the group's political goals. Given that terrorist groups and companies face analogous pressures – including dealing with external "competition," managing internal group dynamics, and preserving a level of "trade secrecy" necessary for their operations – and similar organizational constraints, such an interdisciplinary approach provides both the opportunity to capitalize on an already extant body of scholarship and a novel perspective from which to examine extremist groups.

OVERARCHING LESSONS FROM COMMERCIAL TECHNOLOGY ACQUISITION

Given its clear impact on spheres as disparate as public health, economic development, individual communication, and national security, scholars in many fields have long been interested in technology and how it affects society. For many years, this interest focused on the effects of technological advance, for example, how an industry adapted when a new process

or product was introduced to compete against those dominating a market. From this analytical perspective, the simplifying assumption was often made that new technology came from "outside" the economic system and that, once introduced, it could relatively easily spread from firm to firm, revolutionizing business as it went.[13] Although such an approach produced insights about how technology changes the systems into which it is introduced, by not considering the sources and the *process* of technological change, the lessons learned represented only a partial understanding. In recent years, these assumptions about technology introduction and diffusion have been replaced by the appreciation that the discovery of new knowledge and its spread from organization to organization are very complex processes. Furthermore, the efficiency of these processes can differ markedly for different organizations.

Although examples do exist of the "simple case" where technologies immediately spread and are readily adopted, it is well established that *all* individuals and groups do not absorb and successfully apply new technology at the same rate. To cite one example, while there are companies which have based their entire business plans on electronic commerce and the potential of networked computers, there are others which are still learning to profitably integrate electronic mail or the World Wide Web into their workplace environments. These differences in technology adoption have been observed for many types of technology and persist even when the stakes associated with adopting are very high; for corporations where key technologies changed under them, an inability to absorb and apply the new techniques has led to the failure of the organizations. Because the importance of knowledge for corporate success and national economic competitiveness continues to increase rapidly, a great deal of study has been devoted to identifying the technological characteristics and organizational "roadblocks" which affect the technology acquisition process. The explanation which has been advanced to explain these phenomena is rooted in the observation that the concepts "technology" and "knowledge" – which might be used to refer to things from a simple welding tool to the circuit designs for a supercomputer to the abstract ideas that make up a business strategy – are too general. Closer observation reveals that, within both the business environment of a firm and the military environment of a terrorist group, these concepts must be subdivided and specified before they are sufficiently useful to support conclusions about the discovery or application of new knowledge. It is these issues, which will underlie subsequent discussion of terrorist adoption of military technology, that will be briefly discussed in the remainder of this section.

There are two general mechanisms through which an organization can acquire new technology. One mechanism is to develop the new technology within the firm; this *internal innovation* provides the opportunity for a temporary monopoly on the new knowledge which the organization could use to gain an advantage over its competitors. To one extent or another, all firms have some internal innovation processes as they develop and apply the basic ideas needed to operate in their chosen sphere or market. Alternatively, companies can utilize technology produced by other researchers in the public or private sectors. Companies access these *external* sources of innovation by buying new equipment, purchasing rights to others' knowledge, hiring individuals familiar with the technology, and other routes. In many studies of technology in both the commercial and military spheres, this distinction between internally "developed" knowledge and externally "purchased" knowledge was assumed to fully illuminate the process of technology *application* as well as *acquisition*. In the strongest version of this view, while development of knowledge internally might involve a long process of research, purchased knowledge could be easily transferred into a firm and quickly put to use. This viewpoint is most easily seen in the metaphor of new technology "as a machine:" while developing and building the machine might take a long time, if the machine is purchased it should be immediately plugged in and turned on. More recent studies of technological innovation, however, have shown that the adoption of new knowledge is not so simple. Although a purchased technology may not entail the specific costs involved in developing new knowledge, it is often the case that even well understood technologies do not readily transfer into a firm and are not easily applied.

To explain this observation, scholars of technology have drawn a distinction between different types of knowledge. The first is *explicit knowledge*, information like the recipe for a food product, a scientific protocol, or the blueprints for an automobile which can be readily codified and set down in written form or embodied in a physical object. Because it is easy to "capture" explicit knowledge it is also readily transferred between one firm and another. In contrast, *tacit knowledge* is much more difficult to transfer among individuals or firms. Examples of tacit knowledge include the general "know-how" of engineers used in product design, the understanding of a machine's operation gained by its user through long experience, and a plant manager's intuition about the most critical factors in a production process. Since tacit knowledge is hard to identify, much less codify, transfer is far more difficult. Although a

great deal of the knowledge which underlies an organization is explicit, it is now broadly appreciated that the body of tacit knowledge which exists in an organization is critical for its operation. *It could be argued that it is this tacit knowledge which makes it possible to effectively apply and use explicit knowledge.* This "tacit component" of an organization's knowledge base, which can be quite large, is also very important from the perspective of a company's competitiveness with respect to others in its industry. Because it is difficult to identify, tacit knowledge represents a set of practices and understanding which tend to "stick" to an organization and its personnel – they are hard to appropriate or steal – and therefore are easier to keep secret.

Although the "stickiness" of tacit knowledge can be positive for preserving trade secrets, when organizations want to transfer technology it can be a significant stumbling block. Returning to the metaphor of the machine used above, even if the company selling the equipment makes every effort to communicate its knowledge about usage, much of the tacit knowledge associated with the machine's operation will not be effectively transferred.[14] As a result, the purchaser of a new technology will *always* have to go through a subsequent internal learning process where necessary tacit knowledge is "discovered" and the technology is adapted to the user's specific needs. The extent of this learning process will be related to both the nature of the technology and the characteristics of the firms and individuals involved.[15] If a terrorist group, for example, obtained a fully armed attack helicopter on the arms market, even though the capabilities of the hardware and "instructions" for its operation might be accessible, the group would be unable to use the technology effectively without significant flight training and experience with its weaponry.

TECHNOLOGY ADOPTION IN LEGAL AND ILLEGAL ORGANIZATIONS

The tendency of many terrorist groups to limit themselves to a small range of tactics[16] and their overwhelming preference for operations using only firearms and explosives[17] has led some scholars to discount the desire for innovation among most terrorist organizations. Although there are certain areas of terrorist operations where this characterization may apply, such a broad statement does not consider the critical role which technological advance and tactical improvement have played in many groups' operations and the differences in

technological aspirations which exist among different groups. Many examples exist in the literature of terrorist groups, even those who have restricted themselves to certain weapons, being violently and effectively innovative. Two particularly good case studies are the advances made in bomb-making by the Provisional Irish Republican Army (PIRA) and the numerous operational improvements made by the Red Army Faction (RAF) over the course of their organizational lifetime. In the case of the PIRA, Hoffman has described how the group improved their detonator technology to incorporate first crude timers, then radio control, and finally triggers using radar detectors or remote photographic flash units.[18] In the case of the RAF, the group devoted significant effort to defeating law enforcement's attempts to capture members of their organization. From studies of police tactics and trial transcripts, the group researched ways to thwart the police including developing a special ointment which, when applied to the fingers, eliminated fingerprints. As a result of such innovations, one former member of the group declared that before its cease fire in 1992, the RAF had reached "maximum efficiency."[19,20] From the perspective of threat assessment, the most important question is what made these organizations different from the many other groups that sustained extended "careers" without marked improvements in the tools of their trade.

To facilitate this analysis, the process of technology adoption by any organization can be broken down into two interrelated stages. The first entails the individual or group decision-making process involved in choosing to adopt a new weapon or explore new tactical options. It is during this stage that the hard limits of a group's technology trajectory are defined: if it is unwilling to seek out a new innovation, it is an obvious and inescapable result that the group will never have that new technology to use and apply. Like any decision-making processes, understanding such technology choices requires delineating the many internal and external factors which can influence a group's preferences and perceived constraints. If analysis stops here, however, a significant portion of the technology acquisition process and many factors which can affect the technological trajectory of a terrorist group will be overlooked. In addition to being *unwilling* to adopt a technology, a group may be *unable* to successfully absorb it and gain the knowledge required to deploy it effectively. As a result, understanding the forces which may influence a group's ability to apply technologies is equally critical for accurate threat assessment. Even if a terrorist organization decides and devotes itself to the acquisition and deployment of a particular weapon, if organizational or resource constraints

doom the endeavor to failure, the group's choice to pursue the new technology may result in it posing a reduced rather than an increased threat. The following sections attempts to construct a framework for this more holistic view of technological threat assessment of terrorist organizations by examining the decision process surrounding innovation and the forces which affect the adoption and deployment processes as well.

Stage 1: Factors Influencing the Decision to Innovate

Characterization of the desire of an organization to innovate, whether in the commercial or military realm, begins with a few simple questions. Does the organization seek out new ideas, or is it "satisfied" which its current options? Does it strive to improve upon currently used technologies? When presented with a new technological opportunity, does the organization chose to adopt it? If so, how rapidly does it attempt to absorb the new knowledge? The answers to these questions approach the broader idea of whether or not a given organization is innovative or conservative towards technology. Understanding this first level of the technology adoption process – controlled by the organization's "desire for innovation" – is critical for assessing the likely technology trajectory of a group and is therefore a relevant starting point for a technology-based terrorism threat assessment. Exploring the reasons why an organization might see a need to obtain a given technology, the psychological or organizational constraints that prevent (or require) seeking new tactics or techniques, and the group's perceived constraints on their technology-related decision making provides the opportunity to characterize the likely limits to the group's technology acquisition and place boundary conditions on threat assessment.

Organizations, whether they are legitimate or underground, do not innovate for the sake of innovating. Rather, a company or terrorist group will chose to pursue a new piece of technology because of the belief that there is something to be gained by doing so. Innovation and new technology is not an end in itself but only a means to accomplish other organizational objectives. For commercial firms, it might initially be assumed that the decision parameters regarding a new technology would be straightforward. Within the framework of classical economics, the decision to adopt or pass up a new technology should be based on its effect on the firm's "bottom line." If the technology will increase the firm's net profit, it should be adopted; otherwise, it should be ignored.[21] In addition to the organization's perception of how

a new technology will impact their operational results, other characteristics of a new technique may impact whether it is seen as desirable. A new technology might, for example, have benefits in the safety of the organization's workers or members, result in increased in "productivity,"[22] or be seen as more (or less) reliable than existing options. In addition, the "fit" of the technology with the current operations of the group – whether it is seen as compatible with current skills and assets – will also be very important.[23] Although this view seems to provide a clear and unambiguous guide, in practice it is never so simple because how a technological change will affect a company's profitability can seldom be accurately predicted. This lack of predictability comes directly from the inherent uncertainty associated with any technological change.[24] The level of uncertainty can vary, but it is always present and imposes a degree of risk on any technology adoption project. Uncertainty affects estimates of costs for research activities, the predicted complications of implementing a technology, and the time that it will take before the firm is using the new techniques effectively. On the opposite side of the balance sheet, the profit margin of a new product, the cost reductions associated with a new manufacturing process, and demand for a new technology in the market can be equally difficult to foresee. Such uncertainty means that, except in cases where the financial impact of the technology is either massively positive or negative, such an examination does not unambiguously guide decision-making.

Depending on the nature and mission of the terrorist organization, there are some cases where a new technology's impact is unambiguously positive or negative and an informed adoption decision can be made. These cases are based on the nature of the relationship between the terrorist organization and the constituency or audience for its activities. For a group which is highly dependent on a constituency and therefore concerned with causing the "minimum necessary" level of damage during attacks, adopting and using a highly destructive chemical weapon or biological agent would be catastrophic to the group's "bottom line." These groups would therefore have a strong incentive not to adopt these technologies. On the other hand, a group seeking maximal destruction for the benefit of a divine audience would likely conclude such destructive weapons would be appropriate to their goals.[25] An interesting example of this calculus can be found in the behavior of the LTTE in Sri Lanka. Although it used chlorine gas against a military camp in 1990, it has not used it again; one reason cited to explain this change in behavior is a new concern on the part of the organization to appeal to an

international audience.[26] A similar distinction in weapons choice can also sometimes be drawn based on the geographic area in which a terrorist group operates. If a nationalist terrorist group carries out its operations within its home country – and, therefore, within the communities from which it draws its support – it is likely that the organization will be more restrained in its attacks for fear of alienating its supporters. If that same nationalist group carried out attacks abroad, where its core constituency would no longer be directly exposed to their effects, such "restraints" might no longer apply since the perceived costs and benefits would change.

In the absence of any solid analytical method to guide technology adoption, most of these decisions are made using a sort of organizational intuition that the noted economist John Maynard Keynes called "animal spirits." In his view, any risky investment, whether it is in a new innovation or an overvalued Internet stock, comes out of "a spontaneous urge to action rather than inaction, and not as the outcome of a weighted average of quantitative benefits multiplied by quantitative probabilities."[27] This non-analytical nature of the technology adoption decision has led researchers to characterize the "technology strategies" of firms rather than seeking the "rules" behind the decisions. These strategies depict the "attitude" toward technology of the organization as a whole and therefore address questions like how early in the development of a new technology a firm will chose to acquire it and how enthusiastically the acquisition process will be pursued.[28] The technology strategy of a given firm, for example, might be characterized as "offensive" if it always strives to be the first adopter of new techniques to gain an advantage over competing firms. In contrast, a firm might chose a "defensive" technology strategy by allowing other firms to exploit new technology first. Such behavior could be advantageous if the technology is further perfected or more broadly accepted before adoption by the defensive firm. At the other end of the spectrum, a firm might chose to ignore most new technologies if it doesn't believe that modification of its product will be accepted by the market. This is termed a "traditional" technology strategy. At the risk of anthropomorphizing organizations further, these strategies can be viewed as a group's "self image" with respect to technology – groups which see themselves as "advanced" or "cutting edge" will logically move to adopt new technology more rapidly than those who do not.

Just as commercial firms base their technology strategies on incomplete information and intuitive "animal spirits," technology acquisition decisions by extremist organizations will also be inexact and non-quantitative beyond the simplest cases where the impact is so large or so small that it is readily predictable. It is reasonable to assume, for example, that the specific and attributable benefits of adopting surface-to-air missiles will be no easier for a terrorist group to predict *a priori* than it is for a company to foresee the profit impact of a given manufacturing technology. Due to the many convoluting factors affecting the political influence of extremist groups, in many cases, it may not even be possible to deduce the effect of specific technological changes on the "success" of groups even with the benefit of hindsight. As a result, terrorist groups, like the companies discussed in the previous paragraph, will also likely adopt broader "technology strategies" to guide their technology acquisition activities.[29] The construction of such a strategy, as one would expect, is a non-quantitative process which can be influenced by many psychological and organizational factors. Successfully deducing these factors from the nature of the terrorist organization is one way to characterize the technology strategy of the group and predict what technologies the group is likely to pursue. Four of the factors which have been singled out are the organization's technological awareness, how open it is to new ideas, its attitude toward risk, and the nature of the environment in which it operates.[30]

Technological Awareness

Although seemingly trivial when reduced to a single statement, the fact that no terrorist group can adopt a technology of which it is unaware is a constraint which is potentially very important for some organizations. To learn about the existence of new technologies, groups must be in contact with the "outside world." As a result, any barriers raised between the group and the larger world – including physical isolation, intellectual distance, or lack of contact out of a desire to avoid scrutiny or law enforcement attention – might serve as an impediment to technology adoption. These types of barriers would be expected to significantly impact religious groups and cults which isolate themselves from the world for philosophical (or paranoid) reasons and groups forced deeply underground. If such a terrorist group sequesters itself and prevents all mixing between its members and outsiders, it will likely remain locked at the level of technological advancement it had when its isolation began. In contrast, groups

may isolate themselves from outside society in certain ways but still remain in open technical communication in others. A salient example of this behavior is the millennial cult Aum Shinrikyo which, while setting itself apart from the world, continually sought sources of new technology. Group parameters which impact the level of this "external" communication is the level of recruiting of knowledgeable individuals into the group, the number of group members permitted to actively seek information outside the organization, and whether the group participates in activities specific to the gathering and integration of new knowledge and technology.

One example of prominent public concern about the technological awareness of terrorist organizations is the recent controversy over information being placed on the Internet. Because of its universal accessibility and emblematic representation of modern technology, the Internet stands out as a source of worry in the proliferation of knowledge about explosives and more dangerous weapons technologies. As a result, it is thought that access to the 'net provides a way for groups to increase their technology at low risk. This role in providing technology information could be particularly important for the types of "closed" organizations alluded to in the preceding paragraph; the international scope of the Internet could allow these organizations access to broad sources of information even from the privacy of their own fortified compounds. The ready accessibility of bomb making manuals like *The Anarchist's Cookbook* or *The Big Book of Mischief*, for example, has generated enough fear at the national level that, independent of the free speech implications, US lawmakers have made attempts to ban their dissemination.[31]

Openness to New Ideas

Even if a group becomes aware of a new innovation in weaponry or tactics, if it is hostile to novel ideas or resistant to change there will be no incentive to adopt it. Although the level of such "open mindedness" can be affected by many variables, the philosophical perspective of the group and its leaders and the internal group dynamics of the organization are likely to be dominant factors. Many authors have broadly characterized terrorist groups as "operationally conservative" and generally hesitant to adopt new tactics and methods. This conservatism has previously been interpreted as their desire to succeed at their operations with a minimum of risk[32] (discussed in more detail below) combined with a reticence to make big changes in their modes of operation. Bruce Hoffman has identified a group of "traditional"

terrorist groups (including the PLO, PIRA, ETA, JRA, and RAF) in which this reticence is particularly pronounced.[33] In his view, the operational choices of these groups displayed the organizations' unwillingness to "take advantage of new situations, let alone to create new opportunities."[34] Such an "organizational inertia" that works against new ideas is not unlike a corporation which, over the years, has developed standard ways of operating. Such a reticence was singled out – and labeled the "not invented here" syndrome – as a primary cause for difficulties in the competitive performance of US companies in the 1980s.

In an analogous manner, the longer a terrorist organization exists and the better established it becomes, the more likely it is that expertise in its "current" technologies will be a strong disincentive to replacing them. In addition to the psychological price an organization might pay by displacing a mastered technology with a new one, significant financial costs may also be involved if materials and systems will be made obsolete by the change. For example, the fact that Czechoslovakia reportedly shipped thousands of tons of Semtex plastic explosive to Libya, Syria, North Korea, Iran and Iraq[35] during the 1980s means that groups sponsored by those nations will have a financial and material disincentive to give up explosives as a weapon. Although the level of impact that such an investment will have on states which likely have sufficient resources to ignore the "sunk costs" represented by the material, the accessibility and costs (both direct and perceived) of procuring and using alternate weapons could affect that judgement. In addition to affecting the decision to adopt new weapons, if a significant percentage of the group is "tied" to an older technology, it is much less likely those individuals will actively strive to master a new technique even if it is pursued.

It is invariably the case that the response of any organization to external stimuli, while not fully determined by its leadership, is strongly affected by the characteristics of its leaders and how information is transmitted from the leadership to the remainder of the group. At the simplest level, groups led by individuals who are open to new technology will be much more likely to seek and adopt innovations than those led by individuals hostile to it. Groups whose leaders have technical backgrounds – like Yasser Arafat of the PLO who has an engineering degree, George Habash of the PFLF who was a medical doctor,[36] and Ramzi Yousef, who had a diploma in computer-aided electrical engineering[37] – would be expected to have a greater organizational "desire" to innovate than a group led by a conservative Islamic cleric who has

spoken publicly against modern science. As a result, to the extent that the background and views of individual terrorist leaders can be assessed, those characteristics can be used to help predict the desire to pursue a given course of action.

In addition to these organizational and investment pressures, the philosophical and ideological views of a group – including both the espoused "philosophy" of the organization and the "actual" philosophy revealed by the group's actions – are also critical in determining whether it will seek out new technology. Given that a great deal of analysis has been devoted to how groups' philosophical frameworks affect their operations, one example is sufficient to suggest their effect on technology and innovation. At one extreme there is Aum Shinrikyo whose philosophy and metaphysics specifically included "diagnostic" tests and "scientific" examination as part of cult indoctrination and initiation.[38] Such a viewpoint would clearly predispose the group to inputs of a scientific or technological nature. The writings of Abd Al-Salam Faraj, leader of *Al-Jihad*, have a markedly different view of novelty and new ideas: "The most reliable speech is the Book of God and the best guidance is the guidance of Mohammed…. The worst of all things are novelties and every innovation is deviation and all deviation is in Hell."[39] As a result, it is unsurprising that it was the former of these two groups that sought out and attempted to deploy chemical, biological, and nuclear weapons.

Attitudes toward Risk

One of the central considerations for the terrorist group seeking new weapons or tactics and, therefore, for the analyst seeking to understand that process, is the level of risk which is inherent in any attempt at technological adoption. In the legitimate business world, these risks are financial – the costs of purchasing and adopting a new technique may not be recouped and the company may go out of business. In response to such business risks, for example, it has been observed that smaller companies generally "slow" their technology adoption strategy and adopt gradually to spread risk over time.[40] The risks to a terrorist group, because of the lethality and illegitimacy of its "business," can be significantly higher. The choice to integrate a new technology into a group's repertoire and use it in operations instead of currently "proven" methods entails both the risk inherent in learning a new military technology and the operational risks of failure associated with deploying it. At the most basic level, mastering a new military technique can be physically dangerous. Failures during the process of deploying

bomb-making technology, more than just leading to financial costs, are likely to result in the death or dismemberment of members of the group. It has been estimated that PIRA, for example, in the period from 1970 to 1996, lost approximately 120 members due to accidental shooting incidents or premature explosions. These explosions were most common in the seventies when the group was less experienced and became less frequent as members gained a greater mastery of the technology and learned how to integrate safety features into the devices.[41] Similar incidents have occurred in Mid-East terrorist organizations, including explosions killing Kamal Ismail Hafez Kahil, a leader of the *Izzedine al-Qassam* brigade in April 1995;[42] in March 1998;[43] killing Muhi a-din Sharif, called "The Engineer's Apprentice" for his relationship with the noted *Hamas* bomb-maker in April 1998; in August 1999;[44] and, most recently, in February 2000.[45]

Beyond the obvious "costs" to the individuals involved, these technological failures can also have a significant impact on the terrorist group as a whole. Depending on the value of the members who are lost in the accidents, such individual casualties could be crippling to a group. If an organization lost, for example, its most experienced bomb-maker, the technological capabilities of the group could be decimated by a single "research" accident. For example, in the early seventies, three leaders of the Weather Underground were killed in a bomb mishap.[46] In addition, these types of events can also exert a significant strategic and intelligence cost on an underground organization. An unexpected explosion will almost certainly result in the loss of a safe-house or facility which was part of the organization's physical infrastructure. The investigations which follow the accidents can also provide law enforcement officials with information about the group's activities and plans. An accidental fire resulting from bomb-making activities led to the capture of Ramzi Yousef and his laptop computer which contained his subsequent plans to destroy multiple US aircraft and assassinate Pope John Paul II.[47] It should be noted that the level of these risks an organization is willing to bear is related to the size and resources it has available. Just as a $2 million investment is a very different risk to a ten person company than it is to a multibillion dollar multinational firm,[48] the perceived risk level associated with the same action will almost certainly differ among terrorist organizations.

Beyond the risk of physical and human costs of using new technologies, operational failures or "research accidents" also place the perceived effectiveness of the terrorist

organization at risk. For groups whose success depends on credible threats of future violence, public failure can severely diminish the impact of terrorist actions. If a group believes that they need a "100%" success rate to ensure they gain world attention for their views or agenda, the risk of failure may be a significant stumbling block to the adoption of new weapons technology. Although clear data on the number of terrorist "failures" which have occurred and their effect on the groups involved are not readily available, examples of groups attempting to shift responsibility for mistakes to avoid these perceived consequences do exist. For example, in the afore mentioned 1995 accident that resulted in the death of Kamal Kahil, *Hamas* attempted to blame Israel and the PLO for the bombing presumably to avoid this "loss of face."[49]

Nature of the Environment

In addition to group characteristics, the nature of the environment surrounding an organization also can have a significant effect on how it chooses to pursue new knowledge. From the commercial perspective, the most critical influences exerted by the external environment are the level of demand in the market for the products associated with a new technology and the actions of the organization's competitors. Even if a firm is hesitant to adopt a new innovation, if the customers which that firm serves specifically demand products that incorporate it, the firm will be forced to adopt it. This so-called "market pull" effect has been observed, for example, in the use of sophisticated machine tools in the manufacturing industry.[50] In some cases, the market demand may not be overtly stated but rather exist as social pressure resulting from the overall technological sophistication of the society. If a society is very advanced and places a high value on technical progress, unwillingness to adopt new technology could damage the credibility and position of an organization. In the case of terrorism, this market "demand" is construed to be the requirement that groups ensure their attacks are dramatic enough to warrant media attention and notoriety. One way this has manifested itself is the perceived pressure for terrorist groups to escalate the lethality of their attacks. Timothy McVeigh, discussing the bombing of the Murrah Building in Oklahoma City, was quoted as saying that a "body count" was needed to make their political point.[51] Such an escalation essentially requires adoption of newer, more destructive technologies.

In addition to market pull, the actions of a firm's competitors can also exert a powerful effect on technology acquisition. In a very competitive market, for example, the fear that competitors will gain an advantage using a new technology can overwhelm the uncertainty associated with the costs of innovation and "force" a firm to adopt. A study of banks showed that firms in more concentrated (and therefore more competitive) local banking markets were much more likely to adopt the new technology of automated teller machines.[52] This competitive pressure leads firms to strategize about when in the "technology life cycle" they should adopt a technology. Pursuing a technology early may gain an advantage over competitors but will also require more efforts to "debug" the technology as well; adopting later may be more trouble-free but any competitive advantage might be lost.[53] From the perspective of terrorist groups, this "competitive advantage" is the shock value associated with the first uses of a new weapon. For example, Aum Shinrikyo gained a level of notoriety by using chemical weapons which will set it apart from other extremist groups for many years to come.[54] In balance, it should also be noted that their failure to use these weapons to their full potential demonstrates the risks associated with being an early adopter of a new technology.[55]

In addition to these "customer-driven" influences, terrorist groups also are subject to a category of pressures which lack an analogue in legitimate organizations. For example, the impact of law enforcement and counter-terrorist forces, in addition to affecting operations which are underway, can have a significant effect on a group's technology adoption process. Like the small business owner who lacks the time to investigate new techniques or the leisure to reflect on how new technology might change his or her business plan, a terrorist group under pressure of pursuit will also have a serious disincentive to seek out or attempt to adopt new technologies. The efforts of counter-terrorist forces could push groups toward new technology as well. If law enforcement groups use technology extensively in their attempts to defeat the terrorist organization, this pressure could move the organization to defensively adopt new tactics and weapons in response (see discussion of "the technology treadmill" above.)[56] Furthermore, if the efforts of law enforcement cut off a group from accessible sources of weapons, it may be forced to innovate and devise new ones to continue operations. In the case of LTTE, this pressure operated in reverse. Earlier in its history it lacked access to basic weapons and so pursued tactics like chemical warfare (see above); when standardized military technology became available it had much less of an incentive to innovate.[57]

Stage 2: Factors Influencing Successful Technology Adoption

Although the intent to acquire a new technology is the initiator of the adoption process, making the decision is the easier part of the procedure. Once it is so committed, the organization must move past the point of planning to the second stage of the process and actually adopt the technology. This transition requires that the group devote the resources necessary to purchase or develop the technology and, having made that investment, assume the risk associated with the endeavor. At this point, the question is no longer whether the group is "innovative" or "non-innovative" but whether it will be successful at completing its desired course of action. As a result, *successful* technology adoption becomes a question of effectiveness of implementation in addition to sustained organizational desire. The examination of technology adoption, beyond simply characterizing an activity as a success or failure, can also consider whether a given terrorist organization has the abilities to use a technology up to its full potential. A bomb planted in a building by one terrorist group, for example, might cause few casualties and some property damage while the same device planted by a more experienced group would lead to the collapse of the building and a far more lethal attack. The second group, because of a greater knowledge of explosives and tacit understanding of where to place them for maximal effect, has arguably adopted the technology more completely. As a result, all other variables being equal, the second group would pose a far greater threat and be more worthy of counter-terrorist attention. In light of this realization, it is therefore critical for the analyst to examine the factors and pressures which can affect the chances that an organization will successfully adopt a technology and the probability that it will utilize it to its full potential. Although there is some overlap in the factors which affect organizational decision-making and the likely success of implementing those decisions, this deployment process contains even more inherent stumbling blocks where the intent of the organization can go awry.

Because of the economic impact of technology acquisition activities for commercial firms and the large disparities observed in the decisions and adoption success among companies, a great deal of study has been devoted to understanding the organizational characteristics that affect technology adoption. These characteristics have been characterized in terms of "roadblocks" to successful knowledge acquisition and deployment.[58] It should be

noted from the outset that there is great variation among terrorist groups in these organizational characteristics and, therefore, in their abilities to deploy technology well. As a result, rather than providing general "rules" about technology and all terrorist groups, this framework is more appropriately a method to examine individual organizations. To the extent that these characteristics can be identified *via* intelligence or analysis for specific groups, more informed projections can be made about particular organizations' potential to innovate upon current weapons choices or to seek out and deploy new ones.

The Nature of the Technology

Beginning from the most basic characteristics of different technologies, variations in "inherent complexity" will affect the ability of groups to successfully adopt techniques or devices. At one end of the spectrum, the use of simple firearms and explosives requires very little tacit or explicit knowledge and can therefore be mastered by almost any terrorist. These two routes are arguably the terrorists' 'lowest technology' and 'lowest training' tactical options and it is unsurprising that they have remained popular through the entire history of modern terrorism. Conversely, the construction of a working nuclear weapon, even assuming all the physical ingredients were readily available, would require a broader range and larger amount of scientific knowledge and experience and, as a result, much more effort by a terrorist group. Such a simple argument, based only on the complexity of the knowledge involved, is consistent with the observation that only a single terrorist group, Aum Shinrikyo, is broadly acknowledged to have had a serious program to assemble its own nuclear device.

Although the ability of terrorist groups to produce complex weapons systems internally is restricted by constraints of technological adoption, much of the literature focusing on technology and terrorism considers the "easier" case where terrorists procure such technologies from external sources. If a group can obtain a weapon in a form where much of the required knowledge is already embodied in the hardware – purchasing a timer controlled, fully operational nuclear device as opposed to assembling one, for example – then the chance of the group successfully using a technology which is otherwise "beyond its ability" is greatly increased.[59] Although such weapons systems are readily available to the terrorist organization and do pose a significant threat, the assumption is often made that there are *no* knowledge constraints to their successful use. In reality, even "off-the-shelf" weapons, like a new machine

purchased by a commercial firm, require the accumulation of tacit and experiential knowledge regarding their use. Terrorist use of free flight, armor-piercing missiles to attack vehicles and buildings is one such example. Although a seemingly "simple" weapon, terrorist groups "have generally failed to achieve the clean hit at the right angle in the right place on which hollow charge missiles depend for their effect."[60] Even more dramatically, in 1975, Black September Organization terrorists attempted to destroy an El Al airliner at the Orly Airport in Paris using a Soviet 40mm RPG-7 grenade launcher; as a result of their improper use of the weapon, they missed and hit a Yugoslav Airlines plane instead.[61] Such examples demonstrate that simply assuming that the purchase of a technology implies its successful adoption may overestimate the actual threat posed by terrorist possession of some weapons. This understanding may also help explain why predictions made in the 1980s and 90s that the use of these weapons would greatly increase have not been broadly fulfilled.[62]

Beyond its usefulness as a rudimentary predictor of the ease of technology adoption, this basic distinction between "simple" and "complex" technologies is also useful in predicting whether terrorist organizations will be able to modify and customize a weapon for their unique use. The ability to adapt a technology for unique "local" requirements demands a much deeper understanding than that required to just use the technique or product. If someone wanted to disassemble their video cassette recorder and alter its operation to better suit his or her needs, the level of knowledge required to do so is more extensive than that needed to simply use it to record television programs. All other variables being equal, it will be more likely that a terrorist organization will acquire this level of mastery of simple technologies rather than more complex ones. In light of this distinction, the extensive amount of innovation that has been shown by terrorist groups in the use of explosives, a very simple technology, is not surprising. The basic grenade, an application of plastic explosives mixed with nails or metal fragments and controlled by a short time fuse, is a common weapon that has been made successfully by almost all terrorist groups. Organizations with a greater mastery of the technology have gone beyond basic construction, however. The PIRA attempted to improve on the design with the construction of the drogue grenade – a hollow charge grenade designed to penetrate armored personnel carriers and tanks. The innovation in design is the addition of a kite-like tail to the explosive which is intended to guide the flight of the grenade and force it to strike the target at the right orientation for its hollow charge to penetrate the armor.[63] More advanced adaptations

also include innovations in remote detonation (discussed previously) and the cruelly innovative bomb designs used by groups targeting civilian airliners. Assessment of the level of innovation in bomb design was, for example, a key part of the investigation of the attack on Pan Am flight 103. Other modifications of basic explosives technology by terrorists have also included construction of booby traps, letter bombs, car bombs, and mines for targeting vehicles or personnel.[64] In contrast to the widespread successes that terrorist organizations have had innovating on basic explosives technology, it should be noted that not all seemingly simple technologies are readily mastered. The fabrication of homemade mortars by the PIRA is one such example. Although straightforward in principle, the mortars constructed by the otherwise technically accomplished group have generally proven inaccurate and caused many operational accidents.[65]

In the case of complex "off-the-shelf" systems – such as precision guided munitions or anti-aircraft missiles – this argument can be extrapolated to predict that terrorist organizations will be unable to customize these technologies. This inability serves as a "bound" on the ways these systems could be applied by terrorist groups. As a result, the operational parameters of a missile used by that same organization can be predicted to conform to the original capabilities imparted by the weapon's manufacturer. Although the quality and effectiveness of modern weapons systems makes this foreknowledge insufficient to provide clear ways of defeating attacks using these weapons, it can serve as a guide to countermeasure design which is unavailable for weapons that are more easily modified by the terrorist.

External Communications Links and the Characteristics of Technology Sources

Just as the extent which a group communicated with the outside world had a significant impact on its choice of technology, its communication characteristics will also affect the success of a technology adoption effort. The presence of information conduits into a terrorist organization will significantly impact its ability to secure the necessary additional information needed to successfully deploy technology. In obtaining this auxiliary (often tacit) knowledge, the characteristics of the group's sources of information are critical. Because it has been singled out as a potential source of terrorist know-how, it is worthwhile to explore these parameters with respect to information on the Internet. At the most basic level, the quality of the information which is available from a source is of utmost importance. Although the

Internet does represent an important source of knowledge about terrorist technology, much of the information which is available is of questionable quality. Even though the "free wheeling" nature of the Internet makes bomb-making manuals readily available, those same characteristics mean that the knowledge delivered has likely not been "validated" and could simply be wrong.

In addition to the quality of the information, what types of knowledge are transmitted by a source can also significantly affect the chances of successful technology deployment. Although bomb-making manuals may be easy to download, is important to recognize that the information transmitted in these manuals is *explicit* alone and the tacit and experiential understanding needed to apply the technology effectively is not included. Another example of terrorists taking advantage of a similar source of explicit knowledge was the "scrapbooks" of media reports about successful skyjacking incidents which were kept by aspiring skyjackers in the late 1960s and early 1970s.[66] Beyond the factual information contained in these sources, the additional tacit knowledge that is required will have to be gained through experimentation by the aspiring terrorist, a process which can be more dangerous to the participant (and likely to lead to arrest and prosecution) than to his or her potential targets. One of the authors of an Internet terrorist handbook blew off both his hands while making one of the formulas contained in his own publication. Whether this was due to inaccuracy in the information or a lack of tacit understanding on the part of the author is impossible to tell but it underscores the risks of such technology sources.[67] Further emphasizing the personal danger in acquiring this tacit knowledge, it has been estimated that approximately thirty percent of the deaths caused by homemade explosives are the bomb-makers themselves.[68] In this light, worries about information on bomb-making, the "worst case" scenarios for chemical accidents published online by the EPA,[69] and instructions for chemical and biological weaponry available on the Internet sound very similar to the arguments made over the last twenty years that nuclear bombs could be assembled by "two graduate students from information in the open literature" and would therefore soon be in the hands of terrorists. One reason that assembly of such a weapon by a terrorist group is now considered a low probability event[70] are the significant obstacles which exist in the construction of technology from explicit knowledge alone.

From a threat assessment perspective, sources of technology which are far more worrisome are those where terrorists can either obtain technologies as readily usable, "point and click" devices or those which transfer tacit knowledge and training to the group alongside new technology.[71] Sources which meet these criteria to differing extents are state sponsors, other better-equipped terrorist groups, sympathetic scientists, and members of the international arms market. Because of their desire to sell weapons, arms dealers may have a financial incentive to ensure that their customers are "satisfied" with their operational performance of their products. This could lead to training in their use and a higher probability of terrorists using the weapons up to their full potential; like training by the group on its own, however, such activities will be subject to the pressures of international counter-terrorist activities and, if performed in an "unfriendly" country, might call unwanted attention to the group's location and intentions. Cases also exist of sympathetic scientists or engineers providing technical information to terrorist organizations. Presumably with the intent of pursuing atomic or radiological weapons, the LTTE assembled an extensive database about an atomic energy facility in Madras, India from Tamils who worked in the plant.[72] State sponsorship of terrorist groups has long been appreciated as a source of advanced weapons technology. Beyond simply providing weapons, states also provide a location for the groups to train and access to potential "experts" who are experienced in the use of the technologies. In addition, once inside a friendly nation, the insulation of the group from threat also provides the opportunity to fully evaluate a new technology and integrate it into the organization's operational repertoire. Reflecting these influences, terrorist acts by groups which are state sponsored have been shown, on average, to be eight times more lethal than those by groups without sponsors; although this differences was ascribed to the access to armaments and technologies made available by the state sponsors,[73] it is relevant to consider the effects that state sponsorship can have on the groups' adoption of the technologies as well.

The potential for international cooperation between terrorist groups for operational or ideological reasons has long been a focus of interest. In as early as 1970, a terrorist operation was staged which brought together a Nicaraguan terrorist with Leila Khaled of the PFLP in the hijacking of an El Al airliner.[74] More relevant from the perspective of the current subject, however, is international cooperation which can lead to technology transfer among extremist groups. Similar direct cooperation among commercial firms, both domestically and

internationally, has been the focus of a great deal of attention in technology and management studies. In these studies, the direct communication and face to face contact generated by cooperation between firms have proven to be critical for the efficient transfer of expertise and tacit knowledge. This provides cooperating firms a significant advantage in effectively using explicit knowledge or already assembled technological systems. Previous examples of such cooperation among terrorist groups included Middle Eastern groups training and supplying weapons to European organizations in the 1970s;[75] the staging of "terror conferences" by Islamic radicals or members of the radical right in the United States;[76] and the PIRA passing on its "special knowledge on the design of booby-traps and radio-controlled bombs to other terrorist groups in exchange for services rendered, while at the same time learning new techniques from foreign terrorists."[77]

The Environment of the Terrorist Group

Just as environmental factors strongly influenced the technology choices of a terrorist group, they can also exert a significant effect on the chances of success of their adoption efforts. In the same way that pressure from law enforcement can restrict an organization's choices by preventing it from exploring new technologies, these pressures can also deprive it of the time necessary to adopt them. Successful use of new techniques requires training and, if the risk of coming "above ground" and taking the time to train is too great, they will never be mastered. This kind of pressure in recent months on *Hamas*, including the seizure of their "laboratories" and materiel by Israeli operatives and the Palestinian Authority, has been partially credited with the marked decline in the group's ability to effectively carry out its terrorist program.[78] Increasing pressure from authorities has also been theorized to have sped up the timetable for Aum Shinrikyo's nerve gas attack on the Tokyo subway which resulted in far fewer deaths than could have occurred had the attack been better orchestrated.[79]

Characteristics of Group Leadership and Structure

In addition to affecting technology choice by an organization, the personal characteristics of a group's leadership also influence the chances of adoption activities being successful. If a leader only values "action," for example, the time spent by a group member practicing or "researching" a newly acquired technology would not be positively reinforced.

As a result, when that technology was applied to "action," it would likely be done so prematurely before the group had the chance to master its full potential. In addition to these effects, the internal group dynamics imposed by the leadership can also affect technological innovation and should be considered. In the adoption of a new technology, inevitably there will be problems during early use or difficulties in adapting the technology to better suit the needs of the organization. Such a "debugging" process – the development of the tacit knowledge needed to use the technology well – is highly dependent on the nature of the relationships between group members and between the group and its leader. For example, a leadership style which is intolerant of internal questioning could inhibit the communication necessary for troubleshooting a new weapon or tactical choice; if discussion of problems and solutions is viewed as dissent or criticism of the leader for choosing the technology, no such questioning will occur and the group will lose the chance to optimize its use of the techniques.

Beyond the personal characteristics of group leaders and the dynamics within a group, the actual structure of a terrorist organization can also significantly impact how efficiently new technology is adopted. The observation that good technology transfer in commercial organizations requires extensive face-to-face interactions and hands on training, for example, has significant consequences for underground groups. If a movement chooses to organize itself using a "cell" or "leaderless resistance" model – where small independent groups operate in varying degrees of ignorance about the plans and intentions other group members – technology adoption by the entire movement will be essentially impossible. Large corporations, even those whose members gathered at the same meetings and shared social time with one another, found that transfer of information from one company division to another was far from easy and often took a great deal of effort. In a sense, the cell structure of a terrorist organization is specifically designed to minimize such "inter-group" transfer. In this case the advantages of security and being able to minimize "damage" if a section of the group is compromised prevent the communication of tacit or experiential knowledge among members necessary to allow efficient technological adoption. Although electronic communication over the Internet could partially offset this disadvantage by allowing some interaction among isolated cells, such written communication is limited to explicit knowledge and cannot transmit tacit knowledge effectively.

Availability of Financial and Human Resources

New technology, especially military technology, is expensive. Organizations must raise funds to purchase the materials or weapons necessary for their innovative activities and gain access to the knowledge required to put those materials to work. As a result, terrorist groups which are financially secure, either by having a contributing constituency like the PIRA or being tied to rich state sponsors like *Hamas* and *Hizbollah*, have a distinct advantage. For other groups, alternate sources must be pursued. When explaining a series of bank robberies performed by their organization, the RAF stated they were gathering resources because "only the 'solution of logistics problems' could secure the continuity of the revolutionary organization;"[80] the statement goes further to say that "the technical means could be acquired only in a collective process of working and learning together"[81] thereby explicitly linking the need for resources with the technical capabilities and training needs of the group. Similar statements, including both the focus on group learning and the revolutionary tone, echo modern "cutting-edge" companies' statements as they appeal for investor funding.

In addition to financial assets, a terrorist organization seeking new technology must either possess or gain access to the necessary human resources; the absence of such assets can serve as an insurmountable barrier to successful adoption. Studies done on manufacturing firms, for example, have demonstrated that human resource issues are a central stumbling block for implementing innovations a *majority* of the time.[82] Assessing a group's personnel resources begins with consideration of the "quality" of the organization's current members – their knowledge and technological experience – and what advantages or disadvantages those assets could represent. For example, an organization made up of former Afghan resistance fighters who gained extensive experience with US Stinger missiles during the war against the Soviet Union would be able to apply that experience if they chose to use that technology against commercial airliners.[83] Beyond a group's current stock of human capital, it is also important to consider its ability to recruit new members with appropriate technical knowledge. Aum Shinrikyo, for example, made extensive efforts to gather members in the scientific and technical disciplines so it would have the resources necessary to produce chemical and biological agents. Consideration of this "recruiting dimension" emphasizes the risk posed by technical personnel who were employed in the former Soviet Union;[84] if a terrorist group has the necessary resources to tap into such an international reservoir of talent, many more

technology adoption options will become available and chances of success will markedly increase. It should also be noted, however, that the human resource challenges for terrorist organizations can be significantly more serious than those for commercial firms. Because of the illicit nature of their activities, extremist groups cannot take advantage of the labor mobility which exists among commercial firms; if a group is in need of an expert bomb-maker, for example, it is not straightforward to simply "hire one away" from a competing organization.

In addition to constraints on the knowledge stock of a group's members, limits on their activities can also greatly affect the success of technology adoption efforts. In light of the tacit knowledge and locally specific knowledge required to apply new technology, a firm must also have workers that are able to perform the "research" required to gain experience with the techniques or devices and adapt them to organization's needs.[85] Such experimentation will necessarily consume those members' efforts and the organization must be able to afford the "costs" associated with part of its staff not participating in current operations. It should be noted that although this "learning by doing" is an important component in the successful adoption of new technology, the converse is also true. If an organization does not use a technology regularly, even one which was successfully adopted previously, the potential exists that the group will lose its ability to effectively use it.[86]

Because the nature and quality of human resources are so important to technological adoption and successful deployment, the size of terrorist organizations also becomes an important variable to consider in such a personnel analysis. Throughout history, terrorist groups have varied considerably in size. On the upper end, Aum Shinrikyo was estimated to have as many as 50,000 members worldwide[87] and the Osama bin Laden organization was recently estimated to consist of an extended network of 4000-5000 individuals. In contrast, the Abu Nidal organization was thought to consist of approximately 500 people, the PIRA and ETA between 200 and 400, and groups like the Japanese Red Army or the Red Army Faction between 20 and 30 individuals.[88,89] In the absence of confounding factors, the larger an organization, the more likely its members are to possess the appropriate explicit and tacit knowledge base to efficiently absorb new technology and the more likely it is that the organization can "afford" to devote some of its members to technology acquisition activities. In addition, for small groups, the effect of other barriers, like lack of knowledge, resources and

time, are likely to be magnified.[90] In addition, it has been observed in commercial groups that small organizations are much more likely to rely on external sources of technology rather than developing it themselves.[91,92]

Group Longevity

Just as having a large number of members to experiment with and perfect the use of a new weapons technology is an advantage, groups which use a technology over an extended time will gradually master it and adopt it more fully. The many improvements in detonator technology made by the PIRA (discussed in the opening of this section) would not have occurred if that group had not had thirty years to work on their designs. The life expectancy of many terrorist groups is very short; it has been estimated that 90 percent do not last a year, and 50% of those that survive their first year do not last for a decade.[93] The short life of most terrorist groups could serve as a partial explanation why most operations are relatively "non-innovative." Beyond simply the chronological time which a group exists, the frequency with which the group carries out terrorist operations is also an important consideration. Although significant advance can be made through research alone, it is often only through the actual use of technology that tacit knowledge is acquired and effectiveness is improved. As a result, groups which stage attacks frequently will be more likely to improve their mastery of technology than those which use it only rarely. In recent years, the rise of "free agent terrorism" – groups who contract their services to others independent of the issue or mission – is particularly troubling with respect to this impediment to innovation. Beyond the reductions in ideological constraints on technology choice that these groups may have compared to more traditional terrorist groups,[94] it is also possible that their international scope and flexibility could afford them longer lifetimes and higher operational frequencies to perfect and adopt damaging technologies.

A FRAMEWORK FOR ASSESSING TERRORIST TECHNOLOGY ACQUISITION

The term "innovation" applied to terrorist groups can take a number of meanings across a spectrum of technology acquisition activities. It can refer to an organization pursuing external innovation by obtaining explicit knowledge as written information or as the technology embodied in weapons and, potentially, the tacit knowledge needed to use them both effectively.

It can also denote internal learning processes including both routine "learning by doing" that moves a group toward more complete mastery of a given tactic or weapon and also the development of new knowledge to improve on an existing technology or develop a novel one through experimentation and development. Because of the potential of all these learning processes to increase the lethality and operational spectrum of these organizations, the approaches which terrorist groups take to innovation are critically important to accurate threat assessment.

The characteristics highlighted in this analysis, to the extent that they can be determined for a given terrorist group, provide a way to more accurately predict both the technology strategies of the organization and its chances to implement those strategies successfully. At the technology strategy stage, such an assessment can allow a more reasoned deployment of both intelligence and counter-terrorist resources. A group which is philosophically and operationally closed to new ideas and options will, at most, improve the technologies they already possess through iterative learning and therefore pose a more "bounded" threat than another more innovative group. At the technology deployment stage, collecting data about the forces that influence group adoption efforts provide the analyst with a window into what otherwise is an entirely restricted space – the actual group activities as they learn to use a new tactic or weapon. Although tabulating the attitudes of a leader toward risk and failure, the network of possible technology sources available to a group, and the educational backgrounds of the people involved does not provide a foolproof method of predicting whether a given adoption effort will be successful, guesses informed by such an analysis are far superior to those based on fear and worst case scenarios alone.

In light of this analysis, one might reasonably ask "what are the characteristics of a terrorist group that make it most likely to pursue and successfully deploy new technologies?" The answer to this question is found most readily in the commercial realm in the form of the small, high technology firm. Any group which is tapped into new technology options, open and hungry for new ideas, willing to take risks, not afraid to fail, and driven by its environment to pursue novelty will clearly have the most positive and acquisitive approach toward technology. If that aggressive strategy is complemented by the necessary human resources, collaborations with sources of technology that transmit both tacit and explicit knowledge,

appropriate leadership and structural support, and an environment which provides both enough pressure to force the firm to try many technology experiments and enough leisure to learn from their results, then its technology adoption efforts are likely to be very successful. From the perspective of terrorist threat analysis, it is a fortunate observation that no terrorist groups have truly possessed *all* of these technology reinforcing characteristics. While some organizations have brought together some of them, examples of which are cited in throughout the paper, the nature of terrorist activities and the individuals who are attracted to them make it unlikely that an organization will arise with the innovative power of a high-tech start-up firm. The goal of the analyst, however, is to identify those most likely to present the greatest "innovative threat" so resources can be deployed appropriately.

APPLICATIONS AND IMPLICATIONS OF THE FRAMEWORK

By examining not only the technological aspirations of terrorist organizations but also the inherent obstacles which exist in the process of technological adoption and deployment, the framework described here represents an improved method of performing technology-based threat assessment of terrorist organizations. Such an understanding of the obstacles and diverse pressures groups face when deploying new technology also provides a better way to examine current topics of concern in terrorism – many of which hinge on technology adoption – and craft ways to address them.

Chemical and Biological Weapons: A Technology Adoption Problem. Over the past few decades, one area which seems to have suffered from such "incomplete" technology-based threat assessment is the use of weapons of mass destruction (WMD) by terrorist organizations. After many years where the broad-based assumption was made that WMD were incompatible with the desired goals of terrorist groups, the use of chemical agents by Aum Shinrikyo fundamentally altered the framework of discussion surrounding the issue. Analysts spoke of a "taboo" being broken for terrorists; now that such agents had been used once, a barrier to being the first to do so was gone. Discussions of the topic turned to the seeming certainty that extremist groups would quickly gain such agents from sympathetic states, poorly guarded stockpiles, or by manufacturing them independently and use them for terrorism.[95] Throughout much of the literature, most authors have made the assumption that few technical hurdles stand

between the desirous terrorist organization and WMD. Fortunately, however, there have been few serious imitators since Aum Shinrikyo's attack and, to date, rogue states have been seemingly unwilling to put finished weapons in the hands of terrorists. Grave predictions made as early as 1979, long before the first successful use of these weapons 16 years later, that, "in the very near future, terrorists will be hijacking not aircraft but entire cities or even nations"[96] have not come to pass.

Examining chemical and biological weapons from the perspective of this framework produces some insight into the possible reasons why their use has not spread broadly among terrorist groups. Contrary to the assumptions which exist in much of the literature, chemical and biological weapons are not simple technologies. Recent assessments of the technological requirements associated with making effective chemical or biological weapons,[97] including an in-depth examination of the World War II US biological weapons program,[98] highlight the significant technical obstacles to producing and using WMD. That the subway attack by Aum Shinrikyo, an endeavor supported by an extensive scientific staff and nearly a billion dollars in assets, produced only a small fraction of the potential number of fatalities is suggestive in and of itself that there are significant technological hurdles to using these weapons at their full potential. It is not surprising that the specific delivery requirements and instabilities of chemical and biological weapons would require that groups accumulate a level of experience and a considerable stock of tacit knowledge before the technology could be fully adopted and successfully deployed. The fact that no more damaging incidents have occurred since the subway attack could be inferred to mean that other potential sources of the technology like rogue states – which would transmit the tacit knowledge to the group in addition to delivering the weapon – have not been as forthcoming as was initially feared.

Although Aum Shinrikyo's experience did demonstrate that an underground group can amass the technical resources and expertise necessary to present a credible CB threat, subsequent events have changed the nature of the environment with respect to these weapons. While Aum "got away" with small CB operations and tests which allowed it to begin perfecting its abilities, increased sensitivity to these threats would make such testing far riskier today. Beyond simply testing, the risk inherent in the weapons themselves is also a strong disincentive for groups to even attempt to adopt them. Unlike assembling a bomb, where risk is confined to

those within the potential blast radius, working with chemical and biological agents could put the entire terrorist organization "in harms way."[99] As a result, the potential costs associated with such research could not only cripple the technical resources of an organization but cripple it operationally as well. The experience of the Soviet biological warfare facility, run by a superpower with significant resources, is telling: in an accident in 1979, a plume of anthrax was released resulting in between 100 and 1000 deaths.[100] Because of their sensitivity to weather conditions, CB weapons also have a significant risk of simply failing; this unpredictability could be a very significant barrier based on the psychological characteristics of a given group.[101]

Although other organizational characteristics also discourage use of CB weapons, including the opinions of group members and the fragmented structure of most terrorist organizations, likely the most important barrier is the effort required to prepare and deploy a workable weapon. Most individuals drawn to terrorism want to take direct action rather than use slower, legitimate mechanisms to advance their political or religious agendas. Initiation of a multi-month to several-year research program to perfect a chemical weapon is incompatible with a group which may disintegrate unless it begins its operations immediately. This basic fact, when coupled with the risks inherent in use of highly toxic and virulent agents, represents the most likely explanation for the limited use of these weapons by terrorists and a rationale to expect this limited use to continue in the future.[102]

Implications for Anti-Terrorist Policy. Given the central role of technology in terrorist activities, it is relevant to ask whether this type of "technology focused" analysis can suggest any novel strategies through which such threats might be countered. Although not originally framed in these terms, the technology studies literature does in fact contain insights which might be applicable as part of a comprehensive anti-terrorist and counter-terrorist policy. Because of the economic importance of technology diffusion in the economic realm, a great deal of effort has been devoted to devising strategies to *remove* roadblocks to effective technology use in commercial processes and product manufacture. In the case of terrorism, the policy should strive to do the opposite – ensure that any technological roadblocks which hinder a given terrorist group persist as long as possible and, if practical strategies exist, increase in number and difficulty.

Examining the two stages of technology adoption discussed in this analysis, several "pressure points" can be identified that might serve as sites where the internal decision and learning processes of terrorist groups could be influenced by external means. At the decision-making stage, the choice of a technology is made among known options (the group's technology awareness) in light of some judgment of the risks and benefits of pursuing it. As a result, any efforts which could either limit the technological awareness of an organization or shift its perception of the payoffs and costs of adoption decisions could influence the process. At the implementation stage, the key to successful technology adoption is bringing together the necessary tacit and explicit knowledge to effectively use a new weapon or tactical advance. Any actions which could be taken to interfere with this synthesis process could prevent a group from successfully completing a new technology acquisition.

The United States has long included some parts of such a "technology focused" approach in its anti-terrorism policy. One component is the stance of "technology denial" which the West, and the US particularly, has taken towards regimes like Iraq in an attempt to prevent them from developing accurate missile technology.[103] Such denial includes limiting the spread of US weapons which involve technologies that could be applied to undesired ends (applicable explicit knowledge) and pursuing diplomatic efforts to dissuade other countries from transferring sensitive information. Nuclear non-proliferation efforts have always included attempts to prevent the spread of the hardware involved in bomb and warhead construction. Some other nations, including Israel, have taken a more direct approach to these types of non-proliferation issues by damaging equipment during shipment (thereby destroying the explicit knowledge embodied in it), intimidating firms involved in transferring technology, and even going as far as assassinating members of Iraqi atomic energy commission thereby eliminating any tacit knowledge they possessed.[104] The sanctions which have been held in place around Iraq since the Gulf War have reportedly had an effect on the technological capabilities of the country. The aging of its technical workforce, the removal of opportunities for younger people to pursue training abroad, and the exodus of trained workers have led to significant reductions in the country's knowledge "stocks" and technical abilities.[105]

Beyond such "traditional" policy strategies, a wide range of "technology directed" actions could be envisioned to strike specifically at the technology adoption and deployment

activities of different organizations. Possible actions, admittedly varying in their levels of diplomatic acceptability, could include:

- Pursuit of diplomatic, law enforcement, or military strategies to prevent known terrorist groups from training. Even small operations which increase the risk of such activities could have a significant effect by pushing a group's effective deployment of a technology far enough into the future that the group will disband before employing it[106] or by allowing time for the development of effective countermeasures to the threat. Attention should also be devoted to limiting the number of safe-havens and states friendly to terrorism to reduce the number of areas available for training and tactical experimentation.

- Pursuit of diplomatic or covert strategies to interfere with the recruitment of competent technological workers into known terrorist groups. Such operations would restrict the passage of the tacit knowledge embodied in these individuals and prevent the accumulation of expertise that would facilitate future technological adoption. Amnesties or incentives could be utilized to encourage knowledgeable individuals to leave groups or direct operations could be undertaken to extract key personnel from a group.[107]

- Efforts attempting to reduce the "market pull" effect forcing terrorist towards new technology could be beneficial. Such efforts could include reducing the emphasis and publicity given to new, high technology threats – including the current high profile given to WMD threats. By giving inordinate attention to events, threats, and hoaxes involving new weapons, society encourages the adoption of newer, more destructive technologies.

- Pursuit of covert and publicly announced actions to undermine trust between extremist groups and potential technology sources. Sting operations and programs of infiltration or subterfuge could increase the risk of approaching external sources of information and technology.

- In the event that a group is suspected to be "near" the effective acquisition or deployment of a dangerous innovation, increasing law enforcement pressure on that

group could be used to interfere with the process. Such pressure could force the group to deploy the technology prematurely (and hence less effectively) or, by changing the perceived risk of the activity, cause the group to alter their priorities. Keeping pressure on an advancing group can also deprive them of the time to explore new technology or, once pursued, fully integrate it into their operations.[108,109]

- In an effort to reduce the value or usefulness of explicit knowledge which is readily available, efforts could be made to "contaminate" sources of bomb-making information, for example, with incorrect and dangerous information. The public disclosure of these efforts would serve to increase the risk associated with using such information and could limit the effectiveness of the Internet as a source for such military data. Additional efforts could also be made to specifically assault known groups with misinformation by electronic or human means to hinder their research and development efforts.

- Traditional anti-terrorist operations to obtain intelligence and stop operations before they are initiated can also play an important part in affecting the technological capabilities of a group. If an organization is prevented from using a technology for long enough, the technology will eventually be lost as knowledgeable members of the group are captured or killed and new members cannot gain the experience necessary to master the technology.

Although such activities cannot, on their own, eliminate the threat posed by extremist groups to mainstream society, restricting the technological capabilities of those groups could partially blunt the severity of their attacks. In the case of weapons or tactics which pose the most serious threats, this blunting could prove to make the difference between terrorist strikes which result in hundreds to thousands of casualties and those which are limited to a very few. Even if such "technology-directed" strategies do not represent a comprehensive way of attacking the terrorist threat in its entirety, it has been suggested that in counter-terrorism, like terrorism itself, "the symbolic act can be as important as actual decisive events."[110] One might speculate that, if groups can be deprived of technologies or successfully punished for the methods and

tactics they *seek* to obtain, groups might be discouraged from making similar attempts in the future.

---

[1] The author would like to gratefully acknowledge the input of Anduin Touw, Jerrold Post, Bruce Don, Bruce Hoffman, James Bonomo, Philip Anton, Brian Jenkins, and the paper's reviewers to earlier versions of this work. Any remaining shortcomings are, of course, the sole responsibility of the author.

[2] "We need instruments of destruction which are of little use to the great masses of the barbarians when they are fighting a few lone individuals but which give a few lone individuals the terrifying power to threaten the safety of the whole masses of barbarians. Our powers of invention will thus have to be directed toward the concentration, the homeopathic – as it were – preparation of those substances whose destructive powers physics and chemistry have brought to light, and toward solving the problem of how these substances can be used in a way which minimizes their cost, makes them easy to transport, and diminishes the effort required to propel them." (Heinzen, K. "Murder" *Die Evolution*, Feb-March, 1849 included in The Terrorism Reader. Laqueur, W. and Alexander, Y., eds. (New York, NY: NAL Penguin, 1987) 62-63.)

[3] Hoffman, B. Inside Terrorism. (New York, NY: Columbia Univ. Press, 1998) 180.

[4] Stern, J. The Ultimate Terrorists. (Cambridge, MA: Harvard Univ. Press, 1999) 73-74.

[5] Hoffman, B. Inside Terrorism. (New York, NY: Columbia Univ. Press, 1998) 177.

[6] The need to overcome the physical security measures which have been taken to defeat terrorism has also been proposed as a reason for the escalation. (Simon, J.D. The Terrorist Trap: America's Experience with Terrorism. (Bloomington, IN: Indiana Univ. Press, 1994) 11.) In this case, the argument is analogous to the pressure which anti-terrorism activities exert to stimulate terrorist advancement – the larger bomb is required because the target was hardened just as a guided missile is required if airport security makes it difficult to smuggle bombs onto airliners.

[7] Wilkinson, P., ed. Technology and Terrorism. (London, UK: Frank Cass & Co., 1993)

[8] Clutterbuck, R. Terrorism in an Unstable World. (London, UK: Routledge, 1994)

[9] Stern, J. The Ultimate Terrorists. (Cambridge, MA: Harvard Univ. Press, 1999)

[10] As will be shown below, this choice of a static viewpoint is not unique to studies of technology and terrorism but was a central characteristic of most studies of technology and its effects until relatively recently.

[11] It should be noted that consideration of differences in groups' abilities to effectively adopt and deploy military technology is not new. Examinations of the capability of military forces in lesser developed countries (LDCs) to effectively use sophisticated weapons, for example, have focused on whether LDCs possess the associated knowledge of the tactics, logistics, and system characteristics needed to employ the weapons and can efficiently go through the "local learning" necessary to adapt the weapons to their needs and to modify and upgrade them over time.[Singh, R. "Advanced Weaponry for the Third World" in Science and International Security. P. Arnett, ed. (Washington, DC: American Association for the Advancement of Science, 1990) 73.] The ability to gain this associated knowledge is the basis for the arguments that, rather than choosing the most advanced technologies by default, countries should instead pursue "appropriate technologies."[Singh, R., 79-81] This literature, with its emphasis on the knowledge and institutional requirements necessary for an organization to effectively use a technology echoes arguments made later in this paper. It is important to remember, however, that differences exist between the difficulties legitimate, government supported military groups can have adopting new weapons technologies and those encountered by underground terrorist groups.

[12] Hoffman, B. Inside Terrorism. (New York, NY: Columbia Univ. Press, 1998) 176.

[13] This assumption was based on how microeconomics described commercial firms. In the static construction of supply and demand analysis, technology is a constraint which affects the shape of supply and demand curves but is not an explicit part of the model. The simplification was made that technological change was an exogenous force which affected a company rather than the firm having an active role in the process of innovation. As a result, consideration of how new technology impacted the activities of the firm fit into the analysis (effects of technological change) but the process of discovering new technology or what was involved in a firm adopting new technology were not addressed.

[14] It should be noted that much tacit knowledge is application specific – i.e. the use of a given machine to make one desired product – and, as a result, it would not necessarily be appropriate or necessary for it to be communicated. It is also the case that the amount of necessary tacit knowledge varies from industry to industry.

[15] In addition to costs associated with the tacitness of knowledge associated with a purchased technology, there are also research costs associated with learning what innovations are actually available for purchase. These costs include not only the obvious ones involved in a company appraising itself of the technology "market" but also the costs associated with a firm maintaining a high enough level of technical sophistication to understand how new technology might apply to its business.

[16] Predominantly hijackings, kidnappings, bombings, assassinations, armed assault, barricade hostage incidents, and product contamination (Simon, J.D. The Terrorist Trap: America's Experience with Terrorism. (Bloomington, IN: Indiana Univ. Press, 1994) 348.)

[17] Clutterbuck, R. "Trends in Terrorist Weaponry" in Technology and Terrorism. P. Wilkinson, ed. (London, UK: Frank Cass & Co., 1993) 130-139.

[18] Hoffman, B. Inside Terrorism. (New York, NY: Columbia Univ. Press, 1998) 180-182.

[19] Hoffman, B. "Terrorism Trends and Prospects" in Countering the New Terrorism, RAND Report MR-989-AF, Santa Monica, CA, 1999, 25-26.

[20] A description based on the efficiency of the organization cannot help but echo the discussions of commercial firms in the earlier section.

[21] Hall, P. Innovation, Economics and Evolution. (New York, NY: Harvester Wheatsheaf, 1994) 167-229.

[22] A new technology, for example, might make it possible for a company to use more workers (if labor is inexpensive) or fewer workers. For a terrorist group, a bomb is a technology which allows both an increase in "worker" safety (by allowing a delayed attack) and an increase in productivity by producing a level of violence and destruction that would have required more individuals armed with lower technology weapons.

[23] Chen, R. "Technological Expansion: the Interaction Between Diversification Strategy and Organizational Capability" *Journal of Management Studies*, **33**(5), 1996, 649-666. (and references therein)

[24] Freeman, C. and Soete, L. The Economics of Industrial Innovation. (Cambridge, MA: MIT Press, 1999) 242-264.

[25] Note also that the ability (or lack of ability) to control the extent of some chemical or biological attacks could also dramatically influence a group's assessment of the costs and benefits of their use. For example, if the political position of a group was such that any "collateral damage" associated with an operation was not desirable, then these technologies would likely not be pursued.

[26] Hoffman, B. Terrorism and Weapons of Mass Destruction: An Analysis of Trends and Motivations, RAND Report P-8039, Santa Monica, CA, 1999, 46-7.

[27] Quoted in Freeman, C. and Soete, L. The Economics of Industrial Innovation. (Cambridge, MA: MIT Press, 1999) 250.

[28] Freeman, C. and Soete, L. The Economics of Industrial Innovation. (Cambridge, MA: MIT Press, 1999) 265-285.

[29] This is not to imply, of course, that a terrorist organization actually has a written document containing their "technology strategy" like many corporations might. This concept should be interpreted instead in terms of the terrorist's organizational "self image" with respect to technology.

[30] A discussion of these psychological elements with respect to decision making regarding Internet and information systems terrorism is included in Post, G.M., Ruby, K.G. and Shaw, E.D., "From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism," *forthcoming*.

[31] Amendment 419 proposed by Senator Feinstein of California to the National Defense Authorization Act For Fiscal Year 1998 (Senate - June 19, 1997)

[32] Hoffman, B. "Terrorism Trends and Prospects" in Countering the New Terrorism, RAND Report MR-989-AF, Santa Monica, CA, 1999, 36.

[33] The inclusion of the PIRA and RAF in this list even though their innovativeness in explosives and counter-law enforcement technologies was cited above demonstrates a nomenclature problem in characterizing groups as either "innovative" or "non-innovative." The same terrorist organization can be very innovative in certain areas (the PIRA in explosives, for example) but non-innovative in others (an unwillingness to attempt new tactics that might require different weapons.) As a result, any characterization of an organization as innovative or not is highly dependent on the particular parts of their operational behavior which are the object of study.

[34] Hoffman, B. Inside Terrorism. (New York, NY: Columbia Univ. Press, 1998) 197-8.

[35] Hoffman, B. "Terrorism Trends and Prospects" in Countering the New Terrorism, RAND Report MR-989-AF, Santa Monica, CA, 1999, 14.

[36] Kushner, H.W. Terrorism in America: A Structured Approach to Understanding the Terrorist Threat. (Springfield, IL: Charles C. Thomas, 1998) 31.

[37] Bone, J. and Road, A. "Terror by Degree" *The Times (London)*, October 18, 1997.

[38] See, for example, the group's WWW site at http://www.aum-shinrikyo.com/english/index.htm.

[39] Faraj, A.A. "The Neglected Duty," para. 2. quoted in Rapoport, D.C. "Sacred Terror: A Contemporary Example from Islam" in Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind. Reich, W. ed. (Washington, DC: Woodrow Wilson Center Press, 1998) 103-130.

[40] Raymond, L. *et al*. "Managing Technological Change in Manufacturing SMES: A Multiple Case Analysis" *International Journal of Technology Management*, **11**(3/4), 1996, 270-285.

[41] Anonymous, "Terrorists killed by their own devices" *The Independent (London)*, February 20, 1996. The British describe these incidents with the soccer (football) metaphor that the PIRA "scored on its own goal."

[42] Associated Press, "Terrorist hideout blasted, bomb blew by accident" *Pantagraph*, April 3, 1995.

[43] International Policy Institute for Counter-Terrorism, "Car Explosion kills a Palestinian in Ramallah," http://www.ict.org.il/, March 31, 1998

[44] International Policy Institute for Counter-Terrorism, "Explosion leads to Discovery of Hebron Bonb Factory," http://www.ict.org.il/, August 16, 1999

[45] International Policy Institute for Counter-Terrorism, "Hamas Activists Injured While Building Bomb," http://www.ict.org.il/, February 12, 2000.

[46] Sprinzak, E. "The Psychopolitical Formation of Extreme Left Terrorism in a Democracy: The Case of the Weathermen" in Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind. Reich, W. ed. (Washington, DC: Woodrow Wilson Center Press, 1998) 77.

[47] Shenon, P. "Broad Terror Campaign is Foiled by Fire in Kitchen, Officials Say." *New York Times Current Events Edition*, Feb 12, 1995, 11.

[48] It is also the case that the acceptable "probability of success" needed to make an investment viable for a firm will differ among organizations. (Rosegger, G. The Economics of Production & Innovation, 3rd ed. (Oxford, UK: Butterworth-Heinemann, 1996) 204-206.

[49] Associated Press, "Terrorist hideout blasted, bomb blew by accident" *Pantagraph*, April 3, 1995.

[50] Vonortas, N.S. and Xue, L. "Process Innovation in Small Firms: Case Studies on CNC Machine Tools." *Technovation*, **17**(8), 1997, 427-438.

[51] Quoted in Hoffman, B. Inside Terrorism. (New York, NY: Columbia Univ. Press, 1998) 177.

[52] Hannan, T. H. and McDowell, J. M. "The Determinants of Technology Adoption: The Case of the Banking Firm" *RAND Journal of Economics*, **15**(3), 1984, 328-335.

[53] Technology life-cycle theory pictures the diffusion of a new technology through a market as a sigmoidal curve. At the beginning of the curve, early adopters of the technology gain an advantage over their competition by having access to the "cutting edge" but do so at the price of fixing the inherent problems with a new technology. In the center of the curve, more firms adopt the technology as the problems are worked out and

still gain some competitive advantage. By the top of the curve, where only the slowest adopters still remain to take up the technology, its problems have all been solved but, because the market is nearly fully penetrated, there is little advantage gained by adopting it. [Schroeder, D.M. *et al.*, "New Technology and the Small Manufacturer: Panacea or Plague?" *Journal of Small Business Management*, 1989, 1-10.]

[54] One could argue that the cult also gained a greater share of attention from authorities and swifter enforcement action against members of the group. Such attention is the flip side to this type of "competitive advantage" for illegal organizations.

[55] It is also the case that terrorist organizations, unlike commercial firms, have more "information challenges" with respect to their relative standing among their peers. Companies are in direct competition with one another and have readily accessible metrics like market share to judge their positions. Competition among terrorist groups is less "direct;" they compete for world attention which is far harder to quantify than sales and revenue. As a result, these decisions would be expected to be even more subjective for terrorist groups than for firms.

[56] This point is addressed with respect to information technology in Post, G.M., Ruby, K.G. and Shaw, E.D., "From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism," *forthcoming*.

[57] Hoffman, B. Terrorism and Weapons of Mass Destruction: An Analysis of Trends and Motivations, RAND Report P-8039, Santa Monica, CA, 1999, 47.

[58] Hagedoorn, J. The Dynamic Analysis of Innovation and Diffusion. (London, UK: Pinter Publishers, 1989) 68-74.

[59] A dramatic example of this conversion of a technology from esoteric and technical to broadly consumable is the popularization of the Internet; once a complex computer network was converted to a "point and click" interface, the knowledge required to use it dropped precipitously.

[60] Clutterbuck, R. Terrorism in an Unstable World. (London, UK: Routledge, 1994) 45. One example cited in this source is the attack on the armored limousine carrying US Army General Kroesen in Sept 1981 in Germany. Although the car was stopped at a traffic light and the attack was made at short range, the missile bounced off the trunk and inflicted only superficial injuries.

[61] Wardlaw, G. Political Terrorism: Theory, Tactics, and Counter-Measures. (Cambridge, UK: Cambridge Univ. Press, 1989) 27. This is not, of course, to say that terrorist groups have not perpetrated some dramatic attacks using "off-the-shelf" weapons. For example, Sudanese rebels used a SAM-7 missile to down a Sudan Airways jet, guerillas in Morocco downed an American weather plane, and African nationalists effectively used

antiaircraft missiles to destroy two civil airliners in flight in Rhodesia. [Wilkinson, P. "Terrorism: International Dimensions" in Contemporary Terrorism W. Gutteridge, ed. (New York, NY: Facts on File Publications, 1986) 39 and Hoffman, B. Terrorist Targeting: Tactics, Trends, and Potentialities, RAND Report P-7801, Santa Monica, CA, 1992. 14.] This increased success with anti-aircraft versus anti-armor missiles could be explained, however, by the lower precision of the hit required to destroy an airborne target.

[62] The lack of broad usage of these weapons may also be associated with the degree of dependence it implies on weapon sources. A group which learns how to use shoulder mounted missiles requires a continued supply of those missiles to utilize their expertise. In contrast, a group which learns to make explosives from fertilizer is not as dependent on a specific external source of materiel for their continued operations.

[63] Clutterbuck, R. Terrorism in an Unstable World. (London, UK: Routledge, 1994) 49-50.

[64] Mullins, W.C. A Sourcebook on Domestic and International Terrorism: An Analysis of Issues, Organizations, Tactics and Responses. (Springfield, IL: Charles C. Thomas, 1997) 298-322.

[65] Clutterbuck, R. Terrorism in an Unstable World. (London, UK: Routledge, 1994) 47.

[66] Poland, J.M. Understanding Terrorism: Groups, Strategies, and Responses. (Englewood Cliffs, NJ: Prentice Hall, 1988) 47.

[67] Mullins, W.C. A Sourcebook on Domestic and International Terrorism: An Analysis of Issues, Organizations, Tactics and Responses. (Springfield, IL: Charles C. Thomas, 1997) 300.

[68] Mullins, W.C. A Sourcebook on Domestic and International Terrorism: An Analysis of Issues, Organizations, Tactics and Responses. (Springfield, IL: Charles C. Thomas, 1997) 307.

[69] Burnham, R. “Potential Effects of Electronic Dissemination of Chemical "Worst Case Scenarios" Data” Testimony before the United States House of Representatives, Subcommittee on Health and Environment, Committee on Commerce, May 19, 1999.

[70] Jacobs, S. “The Nuclear Threat as a Terrorist Option” *Terrorism and Political Violence*, 1998, 10(4): 149-163.

[71] Smith, G.D. “Sources of Terrorist Weaponry and Major Methods of Obtaining Weapons and Techniques” in Technology and Terrorism. Wilkinson, P., ed. (London, UK: Frank Cass & Co., 1993) 123-129.

[72] Hoffman, B. Terrorism and Weapons of Mass Destruction: An Analysis of Trends and Motivations, RAND Report P-8039, Santa Monica, CA, 1999, 48-49.

[73] Hoffman, B. Terrorist Targeting: Tactics, Trends, and Potentialities, RAND Report P-7801, Santa Monica, CA, 1992. 9.

[74] Gad, Z. “International Cooperation among Terrorist Groups” in Technology and Terrorism. Wilkinson, P., ed. (London, UK: Frank Cass & Co., 1993) 135-144.

[75] Gad, Z. “International Cooperation among Terrorist Groups” in Technology and Terrorism. Wilkinson, P., ed. (London, UK: Frank Cass & Co., 1993) 137-138.

[76] Kushner, H.W. Terrorism in America: A Structured Approach to Understanding the Terrorist Threat. (Springfield, IL: Charles C. Thomas, 1998) 41.

[77] Wilkinson, P. "Terrorism: International Dimensions" in Contemporary Terrorism. W. Gutteridge, ed. (New York, NY: Facts on File Publications, 1986) 40.

[78] Hamas sources quoted in Karmon, E. “Hamas Terrorism Strategy – Operational Limitations and Political Constraints,” http://www.ict.org.il/, November 19, 1999.

[79] Hoffman, B. Inside Terrorism. (New York, NY: Columbia Univ. Press, 1998) 126.

[80] Horchem, H.J. "West Germany's Red Army Anarchists" in Contemporary Terrorism. W. Gutteridge, ed. (New York, NY: Facts on File Publications, 1986) 201.

[81] Horchem, H.J. "West Germany's Red Army Anarchists" in Contemporary Terrorism. W. Gutteridge, ed. (New York, NY: Facts on File Publications, 1986) 201.

[82] Swamidass, P.M. and Walter, A,M. "A Classification of Approaches to Planning and Justifying New Manufacturing Technologies." *Journal of Manufacturing Systems*, **9**(3), 1990, 181-193.

[83] Kushner, H.W. Terrorism in America: A Structured Approach to Understanding the Terrorist Threat. (Springfield, IL: Charles C. Thomas, 1998) 30.

[84] Stern, J. The Ultimate Terrorists. (Cambridge, MA: Harvard Univ. Press, 1999) 49.

[85] Winch, G.W. "The Dynamics of Process Technology Adoption and the Implications for Upgrade Decisions." *Technology Analysis and Strategic Management*, **9**(3), 1997, 317-328.

[86] Rosegger, G. The Economics of Production and Innovation. (Oxford, UK: Butterworth-Heinemann, 1996) 182-184. Evidence for this effect in terrorist groups is difficult to find, although there is no reason why it

would not occur in such organizations. It is possible that a detailed analysis of groups with hiatus periods in their operations might demonstrate less effective use of technology after a long period of disuse. Such a study is problematic, however, since it is possible that operational "failures" could occur in group actions which never come to public attention and, therefore, would underestimate the effect in question.

[87] Hoffman, B. Inside Terrorism. (New York, NY: Columbia Univ. Press, 1998) 122. It should be noted that this value includes all the followers of the cult and is not an accurate representation of the number of people involved in terrorist and technology acquisition activities.

[88] Hoffman, B. "Terrorism Trends and Prospects" in Countering the New Terrorism, RAND Report MR-989-AF, Santa Monica, CA, 1999, 10.

[89] It should be noted that organization size is a complex variable with respect to technology. Some viewpoints hold that small firms, because of their more limited "organizational baggage" are more nimble than large firms and can more easily switch to new technologies. While this is true and provides an advantage, it is also true that the resource limitations of the firms can pull them in the opposite direction (see discussion of the attitude toward risk above.) As a result, the exact effect of group size on innovation must be examined on a case by case basis depending on exactly what element of the innovation process is of interest.

[90] Vonortas, N.S. and Xue, L. "Process Innovation in Small Firms: Case Studies on CNC Machine Tools." *Technovation*, **17**(8), 1997, 427-438. (and references therein)

[91] Birchall, D.W. *et al.* "Managing Innovaiton in SME's: A Comparison of Companies in the UK, France and Portugal" *International Journal of Technology Management*, **12**(3), 1996, 291-305. (and references therein)

[92] Note that size advantages can only be capitalized upon if the group is organized appropriately. Even with several thousand members, if each group member operates nearly autonomously and communicates little, the group would gain little advantage from its large "formal" size.

[93] Rapoport, D. quoted in Hoffman, B. Inside Terrorism. (New York, NY: Columbia Univ. Press, 1998) 170.

[94] Since they are not as closely tied to constituencies as more "local" or "issue focused groups."

[95] See discussion of this topic in Hoffman, B. Terrorism and Weapons of Mass Destruction: An Analysis of Trends and Motivations, RAND Report P-8039, Santa Monica, CA, 1999.

[96] Clark, Richard Charles Technological Terrorism. (Old Greenwich, CN: The Devin-Adair Co, 1980) 2.

[97] See Stern, J. The Ultimate Terrorists. (Cambridge, MA: Harvard Univ. Press, 1999) 48-68. and Tucker, J.B. and Sands, A. "An Unlikely Threat" *Bulletin of the Atomic Scientists*, 55(4) July/August 1999. 46-52.

[98] Regis, E. The Biology of Doom. (New York, NY: Henry Holt & Co., 1999.)

[99] This is one detail generally overlooked by descriptions of producing infectious agents in a plastic dish in a refrigerator. Without adequate safety precautions, the individual at greatest risk is the potential biological or chemical terrorist.

[100] Englund, W. "Evidence is grim on 1979 anthrax outbreak." *News & Observer (Raleigh)*, February 22, 1998, A14.

[101] Donahue, M. "Terrorist Organizations and the Potential Use of Biological Weapons" in Countering Biological Terrorism in the US: An Understanding of Issues and Status. Siegrist, D.W. and Graham, J.M., eds. (Dobbs Ferry, NY: Oceana Publications, 1999) 22.

[102] Recently, arguments to this effect have begun appearing in the mainstream media questioning the appropriateness of the risk assessments made about biological and chemical weapons and the level of resources devoted to dealing with these "low probability-high consequence" events. (Dobbs, M. "An Obscure Chief in U.S. War on Terror" *The Washington Post*, April 2, 2000, 1.

[103] Arnett, E.. "Technology and Emerging Regional Powers: Implications for US Interests" in Science and International Security. P. Arnett, ed. (Washington, DC: American Association for the Advancement of Science, 1990) 139-40.

[104] Stern, J. The Ultimate Terrorists. (Cambridge, MA: Harvard Univ. Press, 1999) 115.

[105] "Sanctions leave Iraq Short of Brain Power" *China Daily*, February 29, 2000, 4.

[106] It should be noted that if efforts are effective at keeping a terrorist organization "technologically backward" this may increase the probability that the group will disband over a shorter time frame.

[107] Extraction of key individuals (in addition to other, more traditional, military responses) was suggested as a possible response to WMD development in Collins, J.M., Davis, Z.S. and Bowman, S.R. "Nuclear, Biological, and Chemical Weapon Proliferation: Potential Military Countermeasures." Congressional Research Service Report for Congress, 94-528 S, July 5, 1994.

[108] Scott, P. *et al.* "Enhancing Technology and Skills in Small and Medium-Sized Manufacturing Firms: Problems and Prospects." *International Small Business Journal*, **14**(3), 1996, 85- 91. (and references therein)

[109] It should be noted that increasing such pressure on groups can have the undesirable effect of increasing group cohesion and weakening other organizational forces that might cause the group to fall apart. These possible consequences must be weighed against the threat posed by the technological advance before such a strategy is employed.

[110] Simon, J.D. The Terrorist Trap: America's Experience with Terrorism. (Bloomington, IN: Indiana Univ. Press, 1994) 32.