WORKING
PAPER

Organizational Learning and Terrorist Groups

BRIAN A. JACKSON

WR-133-NIJ

February 2004

Prepared for the National Institute of Justice

RAND PUBLIC SAFETY AND JUSTICE

Introduction[1,2]

In the interplay of actors in domestic and international political systems, small groups with intense views on issues or policies have long sought methods to control public opinion and influence the actions of governments. One of the most extreme of these methods, which range from the legitimate and legal to the illegal and violent, is terrorism. Although there is considerable disagreement over the precise definition of terrorism, most authors agree that the tactic consists of the systematic and premeditated use or threatened use of violence by non-state groups for political purposes. Depending on the aims of a particular group, the targets of attack could include physical structures, government representatives, or members of the civilian population. Unlike many other uses of violence, terrorism is intended to have a coercive impact on an audience that is larger than the individuals directly affected by the violent act.[3] By staging attacks that are unexpected and inspire fear in broad groups or populations, terrorist groups can affect public opinion and, as a result, gain a level of influence or control over the policies of states whose size and military might far exceed that of the terrorist organization. These characteristics have led to terrorism being characterized as the "weapon of the weak" and make the tactic, and groups that chose to pursue it, of concern to even the most powerful individual nations and of the international community as a whole.

Although the use of terror and violence is troubling whether it occurs at the local or the international level, the potential for any given terrorist organization to stage operations with far reaching impacts is tied to the group's tactical, strategic, technological, and organizational capabilities. Virtually every day, groups around the

[1] This project was supported in part by Grant No. 2003-IJ-CX-1022, awarded by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. Points of view in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.

[2] The author gratefully acknowledges the input and assistance of Anduin E. Touw, Kim Cragin, and Debra Knopman, Michael Kenney, M. Leann Brown, and Michael Zarkin for input to earlier versions of the manuscript. Any remaining shortcomings are, of course, the sole responsibility of the author. Michael Zarkin.

[3] It should be noted that this definition focuses on the tactic of terrorism. As a result, the definition is independent of the characteristics or aims of any particular non-state group. In this paper, terms such as 'terrorist group' or 'terrorist organization' should be interpreted as shorthand for 'groups choosing to utilize the tactic of terrorism.

world take actions that satisfy the general definition of terrorism. Most of those acts, which include bombings of targets such as pipelines, laboratories, and restaurants or shootings at local government buildings, do not affect actions of governments on the international stage. In contrast, the attacks of September 11th, 2001, clearly demonstrate the potential impact of a terrorist action supported and staged with a high level of tactical and strategic knowledge. Since those attacks, the policies and efforts of the United States government and the most powerful military in the world have had as their central focus responding to the threat posed by terrorist attack. Because the capabilities of terrorist organizations define the bounds of their activities – in the tactics they have to choose from; the amount of damage, death or injury they might cause; and the attention they are likely to command on the world stage – gaining an understanding of the knowledge they have available and how they chose to apply it has long been a goal of policy and military analysts interested in terrorism. In governmental attempts to defeat terrorist operations and arrest the perpetrators, an understanding of what the groups are capable of doing, the types of targets they attack, where and how frequently they can stage operations, and their sources of resources and intelligence information is critical.

A concern with what terrorist groups are capable of doing, however, has embedded within it a question about their ability to learn. Groups do not automatically or immediately gain the ability to use given tactics or carry out particular types of operations. Capabilities must be built. In designing their attacks, selecting their targets, and using technologies for their violent ends, terrorist groups must gather information, integrate it with their past experience, and put it to use. The strengths and weaknesses of these learning processes can not only help explain what a terrorist group is capable of doing today, but also help predict what it might be capable of tomorrow. More importantly, with sufficient understanding of a group's learning processes, new routes may be discovered to interfere and undermine these groups' efforts. Directing analytical attention at this higher level – not at *what* terrorists do, but *how* they learn to do it – may provide a route to gain a new edge in degrading the capabilities of extremist groups and reducing the effectiveness of their attacks.

Organizational Learning and Terrorism Analysis

Like the concept of "terrorism" discussed in the introductory section, there is not a universally accepted definition of the concept of "organizational learning." For example, there is some disagreement surrounding what must occur to demonstrate that learning has taken place, whether the process must be intentional, and if the knowledge gained must be relevant to the actions and goals of the organization involved.[4] For the purposes of this discussion, the following definition (roughly equivalent to that proposed by Miller) will adopted: *organizational learning is a process through which members of a group acquire new knowledge that can be applied in strategic decision-making, tactical planning or design, and operational activities.*

Since organizations only exist as a result of the presence and actions of their members, the process of organizational learning necessarily begins with learning by individual members of the group. Knowledge accumulated by members becomes "organizational" when it is integrated into routines and is institutionalized. The concept of "routines" must be interpreted broadly to include the entire spectrum of knowledge involved in the strategic and tactical activities of an organization. Routines have been defined to include all of "the forms, rules, procedures, convention, strategies,… technologies, …the structure of beliefs, frameworks, paradigms, codes, cultures, and knowledge"[5] associated with group. Organizational routines represent the product of an group's efforts to translate its history and experience into stable and successful methods to accomplish its goals. The conversion of knowledge into routines is critical to constructing an organizational memory where the information is both broadly shared by current members and can be reliably passed on to future members of the group. It is through this process that knowledge or expertise is no longer fully dependant on the presence of particular group members and can survive member turnover and the passage of time.

Concepts like organizational routines are necessarily general in an effort to capture the full range of areas and topics about which organizational learning might take

[4] See, for example, Miller, D. "A Preliminary Typology of Organizational Learning: Synthesizing the Literature" *Journal of Management*, **22**(3):485-505, 1996.

[5] Levitt, B. and March, J.G. "Organizational Learning" *Annual Review of Sociology*, **14**:320, 1988.

place. Organizations learn and create or modify routines relating to topics as diverse as group culture, particular procedures, or esoteric technology choices. However, the significant differences that exist between each of these areas and the differences in the learning processes involved make it very difficult to consider all of them simultaneously. Bringing the full weight of this literature to bear on *all* terrorist group learning activities is clearly beyond the scope of a chapter of this length. As a result, the following paragraphs seek to provide a brief sketch of the range of organizational learning issues relevant to terrorist groups before the discussion focuses more closely on the issue of technological and tactical capabilities introduced in the opening section of the chapter.

Terrorist Group Learning

Although generally not considered as a separate and distinct topic of analysis, organizational learning by terrorist groups has always been an element of the study of terrorism. For example, within the terrorism studies literature, there has been disagreement over whether terrorist groups are innovative or non-innovative organizations. Portions of the literature discount the desire of terrorist groups to innovate and learn since they are generally operationally conservative and usually use a limited set of tactics. For example, over a long period of time, groups have shown a strong preference for staging bombings and firearms attacks.[6,7] Conversely, other authors have characterized terrorist organizations as fiercely innovative, adapting their strategies and routines as a result of external pressures by law enforcement and counter-terrorism forces. For example, the Irish Republican Army gradually evolved their explosive designs to incorporate first crude timers, then radio control, and finally triggers using radar detectors or remote photographic flash units in response to British efforts to jam or defeat their methods of bomb detonation.[8] This apparent disagreement about terrorist innovation results from a focus on the *results* of their actions rather than the learning processes they go through to attain them. The literature on organizational learning – with

[6] Simon, J.D. The Terrorist Trap: America's Experience with Terrorism. (Bloomington, IN: Indiana Univ. Press, 1994) 348.

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

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

its consideration of the different incentives and behaviors that influence their learning efforts – represents a potential source of new insight into these processes within terrorist groups and a route to resolving the seeming contradiction between these two views.[9]

In the context of a terrorist group, the broad concept of learning and the development of organizational routines can be applied to many distinct types of organizational knowledge and decision-making. The topics addressed by these routines can range from the broad strategic level to the most detailed tactical level. At one extreme of terrorist group knowledge lie the overall paradigm that defines and shapes a group's philosophy and world view. A terrorist organization bases its actions and plans on a model of reality derived from a religious, ethno-nationalist, political, or philosophical interpretation of domestic or world events. This philosophical basis is combined with knowledge and ideas about international and domestic political systems, the actions and reactions of governments, and perceptions about the most effective ways for the group to take actions within and against the existing systems. For example, in the case of the left wing terrorist groups active in Europe in the 1970's, such bases included particular visions of Marxism and the assumption that acts of terror could catalyze broader revolution. More recently, for al Qaeda, knowledge at this level includes a radical interpretation of the teachings of Islam and assumptions about how the behavior of the United States might be modified by inflicting casualties on military and civilian targets. This knowledge is developed via organizational processes through which a terrorist organization creates the stories and frames that serve as its "collective understandings of history."[10] Because it is these collective historical interpretations that support a group's decision to engage in terrorism and dictate the types of actions it chooses to pursue, an understanding of the learning processes though which they arise and change could be potentially useful in countering current organizations and discouraging other groups from pursuing terrorism.[11] An example of learning in this

[9] Some recent efforts have sought to include the process of learning into analysis of terrorist group activity. See, for example, Jackson, B.A. "Technology Acquisition by Terrorist Groups: Threat Assessment Informed by Lessons from Private Sector Technology Adoption" *Studies in Conflict and Terrorism*, **24**: 183-213, 2001.

[10] Levitt, B. and March, J.G. "Organizational Learning" *Annual Review of Sociology*, **14**:324, 1988.

[11] Because of the psychological dimensions of these "conceptions of reality" and the learning processes involved in changing them, this area provides the opportunity to combine the lessons of the

area can be found in the Revolutionary Armed Forces of Columbia (FARC) which altered its strategy from a strongly anti-state purely military orientation to presenting itself and structuring its activities to portray itself as a legitimate alternative to the Colombian government.[12] Other examples of such strategic learning can be found in al Qaeda which altered its recruiting practices to include multiple branches of Islam as it transitioned its activities toward a global perspective[13] and the Egyptian Islamic Jihad's shift in targeting institutions and individuals within Egypt to attacking U.S. and Jewish institutions internationally based on their assessment of the effectiveness of their activities.[14,15]

At a slightly lower strategic level, organizational routines also define the types of activities a group will undertake, based on its beliefs about the most effective ways to further of its particular goals. For example, some groups are "pure" terrorist organizations whose activities include only military activities such as bombings or kidnappings. In contrast, other groups take on much broader roles including providing social services to the civilians whose cause the terrorist activities are intended to advance. In the Middle East, for example, groups such as Hamas and Hezbollah maintain schools and other social support services in addition to their violent activities.[16] In Columbia, FARC has also taken on social services roles as its strategy has shifted.[17] Since

organizational learning literature with the body of work in political psychology addressing why individuals or groups turn to terrorism. (Reich, W., ed. "Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind" (Washington, DC: Woodrow Wilson Press, 1998))

[12] Ortiz, R.D. "Insurgent Strategies in the Post-Cold War: The Case of the Revolutionary Armed Forces of Columbia." *Studies in Conflict and Terrorism*, **25**:131, 2002.

[13] Gunaratna, R. Inside Al Qaeda: Global Network of Terror (New York: Columbia University Press, 2002)100.

[14] al-Zawahiri, A. "Knights under the Prophet's Banner" *Al-Sharq al-Awsat*, December 4-7, 2001.

[15] An additional "special case" of such strategic learning can be catalyzed when a group achieves the goals that it has set out to accomplish. If the group wishes to continue its operations, it must revise its worldview to construct a strategic context in which to operate. An example of this process can be found in Hezbollah. Throughout its operational history, the stated goal of Hezbollah was to expel Israeli military forces from Lebanon. With the pullout of the Israeli Defense Forces in May 2000, this goal was achieved. Rather than declare victory and cease operations, the group has since redefined their activities in the context of the Palestinian conflict and continued terrorist operations. (See, for example, Stroumsa, R. and Baidatz, Y. "From Sheba'a to Al-Quds: The Evolution of Hizballah" Peacewatch, 300, December 15, 2000. http://www.washingtoninstutute.org/watch/Peacewatch/peacewatch2000/300.htm (Last Accessed: Sept 14, 2002))

[16] See, for example, Rosin, H. "School May Be Out in West Bank; Crackdown Threatens Respected Hamas-Run Institution" The Washington Post, December 31, 2001, A14.

[17] Ortiz, R.D. "Insurgent Strategies in the Post-Cold War: The Case of the Revolutionary Armed Forces of Columbia." *Studies in Conflict and Terrorism*, **25**:131, 2002.

encouraging these other more constructive activities may be a reasonable goal of counter-terrorist policy, understanding the construction and modification of these routines and the group capabilities needed to support non-military roles and activities could clearly contribute to effective policy design.

Moving away from the philosophical and strategic concepts driving particular terrorist groups, at the other extreme of the terrorist group knowledge "spectrum" lies the detailed factual information needed to carry out individual operations. In military terms, this knowledge is the tactical intelligence involved in selecting a target, planning an attack, identifying and avoiding obstacles to operational success, and, if it is called for in the group's strategy, allowing the attackers to escape. Developing this information is a learning process that seeks to collect and interpret data about the world at a very high degree of resolution.[18] Like security organizations in national governments, the intelligence development process of a terrorist organization relies on particular learning processes that define what information is desired, how much and how current it must be, how it is interpreted, and the ways the finished intelligence influences operational planning and decision-making. For example, the Abu Nidal Organization (ANO), a violent Palestinian group that splintered from Yasser Arafat's Fatah, devoted considerable resources to intelligence gathering on targets. The organization's Intelligence Directorate reportedly maintained operations in dozens of countries monitoring security measures and collecting information on potential targets.[19] For obvious reasons, a more complete understanding of those processes could make a contribution to counter terrorism by suggesting strategies to disrupt or discourage attacks by frustrating this type of detailed and operational organizational learning.[20]

Returning to the area introduced in the opening section of the chapter, the knowledge that supports a terrorist organization's use of particular attacks and weapons

[18] Examples can be found in the literature which label such a process as "learning about" in contrast to "learning how." (for example, Breslauer quoted in Levy, J.S. "Learning and Foreign Policy: Sweeping a Conceptual Minefield" *International Organization*, **48**(2):292.) While this is a relevant distinction, it is often a difficult one to make cleanly. An organization "learns about" reality (a particular target, for example) through some sort of learning process (intelligence gathering). That process could itself be improved, however, at which point the group would be "learning how" to better "learn about" potential targets or likely security obstacles.

[19] Seale, P. Abu Nidal: A Gun for Hire (New York, NY: Random House, 1992) 23, 185-191.

technologies falls somewhere between these two extremes of strategic and tactical knowledge. These routines combine both sorts of considerations and address a range of questions about the particular characteristics of the group's operations: What targets will the group attack? How does the group prepare for an attack? How is the attack carried out? What tactics and weapons are used? *How* are they used? Beyond the particular details of attacks, a body of routines will also govern the internal practices of the group in the induction, training, and use of group members. Are there standardized processes associated with bringing new members into the group? How are they trained? What is required of them? Is there a standardized body of knowledge they are provided or taught? Whether they are aimed at personnel or operational plans, the routines addressing these topics are intimately tied to the capability of a group and the ways they use particular technologies in their activities. As a result, organizational learning processes aimed at altering or improving routines in these areas will potentially advance a group's ability to use new weapons, carry out new attacks, or perfect their skill and expertise in already fielded tactics and techniques. The learning process associated with this class of knowledge can be broadly labeled "technology adoption" and is the focus of the remainder of the chapter.[21]

Technology Adoption: Learning of Particular Concern

In the assessment of terrorist capabilities, a group's technological sophistication and tactical expertise to a great extent define the lethality, scale, and effectiveness of the organization's attacks. The level of access a group has to technology – from the lowest level of basic firearms to the upper limits of weapons of mass destruction (WMD)[22] – define the boundaries for its operations. The level of skill in using any given weapon or tactic then contributes to what fraction of the maximal effect a group might obtain when it uses a technology or operational scheme. For example, a given bomb could be placed

[20] An explicit consideration of organizational learning in this context could provide an opportunity to bring in the literature and scholarship on terrorist operational activities from the intelligence perspective.

[21] For a more lengthy treatment of this topic, see Jackson, B.A. "Technology Acquisition by Terrorist Groups: Threat Assessment Informed by Lessons from Private Sector Technology Adoption" *Studies in Conflict and Terrorism*, **24**: 183-213, 2001.

[22] Weapons of mass destruction are generally defined to include chemical, biological, nuclear, and radiological weapons.

in many different locations by a group targeting an individual building. Depending on the level of tactical, engineering, intelligence, and other types of knowledge available to the group, the same bombing could range from a mere nuisance to a highly lethal terrorist attack. Technology adoption is the organizational learning process through which groups learn about technologies or techniques that might be useful to them, acquire them, integrate them into group operations, and train or experiment sufficiently to use them well. As such, it is the necessary process for groups to upgrade their skill in their current attacks, transition from more basic to potentially more lethal technologies, develop or deploy WMD, and improve their ability to operate in the face of law enforcement and counter intelligence pressure. Therefore, it is a process that must be a constant and central focus in terrorist threat assessment and counter-terrorist planning.

Studies of commercial organizations acquiring and using new technologies have demonstrated that the organizational learning required can be very difficult and its success is not assured. Although examples exist of technologies which a broad range of organizations can learn to use well, there are also ready cases where groups that were provided with the "recipe" for a new technology but could still not use it effectively. Understanding the potential differences in the learning experiences of organizations as they seek new technologies has been a central element in the studies of commercial firms and is becoming increasingly important in studies of illicit and terrorist organizations.

In studies of technology-related learning in organizations, scholars have sought to better explain the process of acquiring and learning to use new technologies by drawing a distinction between *types* of knowledge that are involved. The first is *explicit knowledge*, information or data that can be readily written down or embodied in physical objects. Relevant examples of explicit knowledge include blueprints for a building a terrorist group is seeking to target or a weapon obtained by the group. The second type is *tacit knowledge*, generally unrecorded expertise such as internal "know-how" developed by individuals through experience or implicit organizational knowledge about how techniques or technologies are best used for particular purposes. Terrorism related examples of tacit knowledge include the intuition developed by soldiers over their operational careers and the expertise needed to be considered a marksman with a firearm in contrast to the basic information needed to simply fire it. In contrast to explicit knowledge, which is easy to transfer among individuals or groups since it can be encoded in written form or as technological objects, tacit knowledge is much more difficult to transfer. Since it is often too difficult (or even impossible) to codify tacit knowledge, transfer may require face-to-face communication and hands-on contact to move the knowledge from one individual to another. An organization must bring together the necessary tacit and explicit knowledge – the explicit recipe for the explosives, the tacit knowledge required to manufacture them safely, the explicit engineering knowledge needed to place them well, and the tacit operational expertise to successfully carry out the operation – before they will be able to use a technology most effectively.

Because of the effect of technological sophistication on the impact of terrorist attacks, understanding the learning processes through which that expertise can increase is critical. Gaining such an understanding is not straightforward, however, because of the many different knowledge and technology sources that can be involved in a group's technology adoption efforts. Relevant learning processes include obtaining explicit knowledge from available sources of codified information, acquiring needed explicit or tacit knowledge from other organizations or individuals, and developing relevant tacit or explicit knowledge internally within the terrorist group. These processes can involve organizational search activities, seeking both relevant existing knowledge or appropriate knowledge sources, communication and acquisition activities to obtain knowledge from these external sources, or trial-and-error experimentation.

Search activities may be directed at particular problems encountered by groups but can also be initiated without a clearly defined tactical problem in mind. Because of their illicit nature, terrorist organizations must constantly devise new and better methods to avoid law enforcement or intelligence penetration of the group. In addition, anti-terrorism measures taken at terrorists' potential targets can also present problems that become the subject of group search activities. Setbacks from diplomatic buildings or more rigorous border security, for example, can lead terrorist groups to explore larger explosives or stand-off weapons to either overpower or circumvent the obstacles. The example of IRA explosives innovation in response to improvements in countermeasures cited earlier is a prime example of such problem directed search. On the other hand, some terrorist search activities are not problemistic. Research seeking to acquire certain types of weapons, including chemical or biological agents, is often motivated for reasons independent of particular tactical challenges.[23] This discussion of technological learning is intended to capture both these types of search activities.

The particular characteristics of the knowledge sources identified by the group, the nature of the technologies it is seeking to acquire, and the particular learning processes it undertakes will have a determining effect on the chance that the organization will successfully gain the needed tacit and explicit knowledge to use a particular technology effectively. In addition, these factors will also impact what counterterrorist strategies may exist to allow external intervention and interference in the group learning processes.

Routes of Learning

Learning relevant to terrorist group technology adoption can occur through intentional activity – *via* processes of research or search – or incidentally as the group undertakes other actions or activities. In addition to learning from their own actions, groups can also obtain knowledge from other groups involved in similar or related activities. These information and technology diffusion processes may or may not require the intentional action of members of both groups. Both routes of learning could lead a group to improve on or become more expert in a technology or tactic it already possesses (incremental innovation) or to develop or discover a new technology or tactic of which the group was previously unaware (radical innovation).[24] Returning to the language of organizational routines included above, improvements in current routines (or increasing how effectively they are implemented) could be labeled incremental innovation while seeking out and adopting new and different routines could be considered radical innovation. In the case of tactical use of technology by terrorists, incremental

[23] See, for example, Anonymous, Through our Enemies' Eyes: Osama bin Laden, Radical Islam and the Future of America (Washington, DC: Brassey's Inc., 2002) 66.

[24] The terms incremental vs. radical innovation are drawn from the technology studies literature and are usually used in reference to products or process technologies used in commercial organizations. An incremental innovation, for example, might be a change that improves the characteristics or performance of some part of an already sold product while a radical innovation would be the development and introduction of an entirely new product. While applying these terms to the weapons or tactics of terrorist organizations may not be entirely appropriate from the perspective of this

innovations could include learning how to perform a given operation (kidnapping, bombing, etc.) more effectively, at less risk to group members, or in ways that gain more publicity and put more pressure on the group's intended audience. Examples of radical innovations would include more drastic changes such as using an entirely new weapon (such as portable anti-aircraft missiles or WMD) or beginning to use a tactic the group has never used before. The most obvious recent example of radical operational innovation by a terrorist group was the use of airliners as weapons on September 11, 2001.

Learning by Doing

With respect to organizational learning, a major area of interest is how knowledge and performance improves in the course of routine activities. In commercial organizations, this improvement in performance from experience is labeled "learning by doing." Understanding this learning process has long been recognized as critical for good decision-making and strategic planning. The progress of such learning activities is often plotted in learning or experience curves relating performance variables, such as increasing productivity or decreasing costs, against the number of units produced by a firm or other measure of operational experience. Learning by doing may be inadvertent learning – accumulation of knowledge as a byproduct of activities rather than their intended outcome – or elements of those activities may be intentionally designed to promote learning. Because learning by doing focuses on already adopted technologies and organizational routines, this learning route is more likely a source of incremental innovations than major shifts in group operations and capabilities. Although such learning may involve development of new explicit knowledge related to a particular tactic or attack, generally learning by doing is predominantly focused on developing the tacit knowledge needed to a particular technology closer to its full potential.[25]

literature, the analogy is useful to draw the distinction between the different effects of the learning processes.

[25] It should be noted that the converse of this process, "Unlearning by Not Doing" is relevant in organizations as well. If particular technologies or routines are not used for extended periods, the group will gradually lose the tacit knowledge needed to execute them successfully. This loss of expertise or degradation in the ability of the group to retrieve the relevant organizational routines is particularly relevant in the design of counter-terrorist programs.

In the context of terrorist organizations, this route of organizational learning implies that groups will become more expert with particular tactics and technologies as they accumulate relevant operational experience. The potential for groups to learn during their operations makes it clear that understanding the impact of a group's longevity and its operational tempo on tactical expertise should be included in judgments about the threat posed by particular organizations. All other variables being equal, a group which has a longer operational history with a particular tactic or weapon would pose a greater threat than one that has only adopted it recently.

Despite the fact that learning by doing can build group expertise without requiring intentional activity or resources devoted specifically to learning, there could be a significant risk for terrorist organizations that chose to rely solely on this route of learning. Each individual terrorist operation, in addition to representing an opportunity to learn and refine operational routines, also represents an opportunity for group operatives to be captured or killed and the security of the group compromised.[26] As a result, relying only on learning by doing to improve group performance could be a costly strategy as failed "experiments" in tactical or weapons innovation have to be paid for through large human or organizational costs. In the particular case of suicide operations, the members of the group involved in the action will be lost by definition. As a result, for groups that use that tactic, operational experience must be built in group members who are not directly involved in the operations themselves. This would require separating planning activity from the operational group members and devising routes for the planners to observe or gather data about the success of the actions that did not depend on them being present during the attack. Al Qaeda has developed a number of routines that help reduce the costs of this learning including having overt group members perform certain tasks that might compromise the more valuable covert members of the group[27] and evacuating important members of cells from operation areas before an attack occurs.[28]

[26] Aase, K. and Nybø, G. "Organizational Knowledge in High-Risk Industries: What are the Alternatives to Model-based Learning Approaches?" http://www.alba.edu.gr/OKLC2002/Proceedings/pdf_files/ID465.pdf (Last Accessed: Sept 17, 2002)

[27] Gunaratna, R. Inside Al Qaeda: Global Network of Terror (New York: Columbia University Press, 2002) 77.

[28] Bergen, P.L. Holy War, Inc.: Inside the Secret World of Osama Bin Laden (New York, NY: Simon and Schuster, 2001) 110, 115.

Learning through Training

Rather than simply relying on operational activities to produce the knowledge needed to improve group performance, many organizations take specific actions where knowledge production is the primary (or only) goal. For military organizations such as terrorist groups, training activities are a central part of these intentional organizational learning activities. Operational training is the analog of learning by doing, but because techniques and strategies are tested under more controlled or simulated circumstances, the consequences of failure can be significantly reduced. For example, in the case of a terrorist organization perfecting a new tactic or mastering a new weapon, training is a chance to evaluate or "debug" the innovation away from the pressure of an active operation. Controlled training can also be optimized to allow more learning in a shorter time than relying on incidental experience building.

Such training under more "relaxed" circumstances can result in developing greater expertise in a given technology (learning to execute given routines better), developing new strategies to use the technology (making incremental modifications to routines to take better advantage of its strengths), or developing entirely new routines around the technology (radical innovations in tactics.) These learning activities can involve creation of new explicit knowledge but, like learning by doing, are often associated with development of the tacit knowledge needed to use the technologies well. Depending on the technologies used by the group, explicit knowledge developed in training can allow a broader spread of information through an organization. The al Qaeda training videos discovered in Afghanistan demonstrate the potential for this type of technology mediated information spread.[29]

Although the risks associated with training are less than learning about new technologies and tactics through operations alone, they are far from zero for illegal organizations. In order to train with military technologies, groups must generally come "above ground" and, as a result, potentially call the attention of intelligence and law enforcement personnel. In contrast to learning skills such as document forgery which could be done completely in hiding, training with explosives or chemical weapons

[29] http://www.cnn.com/SPECIALS/2002/terror.tapes (Last Accessed: Sept 8, 2002)

necessarily calls attention to the location and activities of a terrorist group. This underscores the importance of directed intelligence or law enforcement pressure in impeding the learning processes of terrorist organizations. If such pressure increases the risks of coming above ground, groups may be prevented from increasing their expertise in certain areas. Areas or situations – such as the presence of states with governments friendly to terrorist groups or areas otherwise isolated or protected from external pressure – become particularly important in this context. For example, ANO carried out extensive training with its new recruits covering a broad range of military and clandestine techniques involving considerable operational activity. This was only possible because of the organization's access to a desert camp in Libya where the training could be carried out away from external pressure.[30] More recently, the expertise of the al Qaeda fighters in Afghanistan was bolstered by their ability to train under the protection of the Taliban regime.[31] By preventing pressure on groups, state sponsors or safe havens can give groups the opportunity to learn and advance.

Learning through Organizational Research Activity

Beyond training activities, which are aimed at increasing expertise or perfecting routines associated with a group's current technologies, organizational research processes are a route of learning that can also develop or integrate new and more radical innovations into an organization. These processes of organizational search may only consist of attempts to determine what technologies are available, how to obtain them, how they might be used, and what organizational routines might need to be developed or modified to take advantage of them. These search activities focus mainly on identifying sources of explicit knowledge (the technologies themselves) and developing the tacit knowledge needed to utilize them. Organizational research activities may also seek out existing sources of tacit knowledge – generally in the form of individuals or groups that can instruct the group in the use of a technology. This potential effects of this search activity are addressed below in the section on "learning from others."

[30] Seale, P. Abu Nidal: A Gun for Hire (New York, NY: Random House, 1992) 3-24.

[31] Chivers, C.J. and Rohde, D. "Turning Out Guerrillas and Terrorists to Wage a Holy War." *The New York Times*, March 18, 2002, A1.

In addition to seeking out other sources of knowledge, organizational research can involve more "traditional" technology development activities – producing both the explicit and tacit knowledge needed to accomplish a particular goal inside the organization. Activities in this subcategory range from the manufacture of explosives (which is relatively common among terrorist groups) to the production of chemical or biological weapons (which has fortunately been uncommon to date.) Such research activities likely start from some sources of explicit knowledge in combination with any explicit or tacit knowledge already possessed by individuals within the group. For example, explosives manufacturing information available on the Internet could the jumping off point for a group effort at adopting explosives technology. It should be noted that, when these research efforts involve potentially lethal technologies, they are not without risk. Bomb-making instructions do not come with the tacit knowledge needed to use their recipes safely and, by one estimate, approximately 30% of the people killed with improvised explosive devices were the bomb-makers themselves.[32] Terrorist organizations including the Weather Underground, the IRA, Hamas,[33] the Red Brigades, and the Nuclei Armati Proletari (NAP)[34] all lost group members to such accidents. One can imagine that the potential losses associated with nuclear, biological, or chemical weapons could be a significant deterrent to many groups.

In addition to potentially losing group members to research accidents, illicit groups may also compromise safe houses or other hiding places if failures are significant enough to attract the attention of authorities. Such compromise could result in major damage to a group's operational security. One example of such an incident was the discovery of Ramzi Yousef, the mastermind of the 1993 World Trade Center bombing, as a result of a bomb making accident in his Philippines apartment. Information gleaned from his laptop computer during that raid compromised a plan to destroy multiple

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

[33] Jackson, B.A. "Technology Acquisition by Terrorist Groups: Threat Assessment Informed by Lessons from Private Sector Technology Adoption" *Studies in Conflict and Terrorism*, **24**: 183-213, 2001 and references therein.

[34] Drake, R. The Revolutionary Mystique and Terrorism in Contemporary Italy. (Bloomington, ID: Indiana University Press, 1989) 6, 30.

airliners in flight.[35] The loss of the NAP member mentioned above also resulted in the compromise of many documents and arrests of group members.[36]

While training and learning by doing are frequently more important in perfecting current tactics, structured group research activities have a much greater potential to add new technologies and new options to a group's operational arsenal. Because of the potential to introduce radical innovations that could significantly change and improve the effectiveness of a group's attacks, it is understandable that developing intelligence information and indicators for groups' activities in this area is of considerable importance in counterterrorism.

Learning from Others

In all of the earlier routes of learning, the focus of attention was on the internal activities of a terrorist organization. A main component in all three mechanisms was the internal development of the tacit knowledge to either use an externally acquired or internally developed technology or tactic effectively. As a result, development of this tacit knowledge was always a "learning roadblock" to a terrorist organization using a particular technology or tactic to its full potential. Because face to face communication or interaction between terrorist groups and knowledgeable individuals has the potential to remove that roadblock to using technology effectively by allowing transfer of tacit knowledge. As a result, such interactions where terrorist groups learn from others have always been of particular concern.

Potential groups where terrorist organizations might gain such knowledge include individuals associated with state sponsors of terrorism, other terrorist organizations, displaced scientists or engineers with relevant military knowledge, and participants in the international arms market. There has been evidence of cooperation between terrorist groups in training, technology acquisition, and actual terrorist operations activities for many years.[37] For example, through its history, FARC has collaborated with both the

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

[36] Drake, R. The Revolutionary Mystique and Terrorism in Contemporary Italy. (Bloomington, ID: Indiana University Press, 1989) 30.

[37] Wardlaw, G. Political Terrorism: Theory, Tactics, and Counter-Measures, 2nd Ed. (Cambridge, UK: Cambridge University Press, 1989) p.55.

Japanese Red Army and the Provisional Irish Republican Army to gain training and expertise in urban terrorism and explosives respectively.[38] Such cooperation between al Qaeda and Hezbollah has been of particular concern recently.[39] Because of the very significant knowledge and other resources they might make available to terrorist groups, learning relationships between terrorist organizations and states are particularly worrisome. Over a period of some years, terrorist operations associated with state sponsored groups were considerably more lethal than those of non-state sponsored groups. Although this has been ascribed in the literature to the increased access to some weapons technologies provided by states, the contribution of other knowledge and learning resources could also play an important role.[40] Gaining needed tacit knowledge from other organizational or individual sources is much faster than developing the it internal to a group; for many military technologies, it is much safer as well since it eliminates much of the risk associated with experimenting with a new and dangerous technique or weapon.

Obstacles to Learning

During all the learning processes discussed above, organizations make judgements about their efforts based on measures of the outcomes of their actions. These measures lead to conclusions about the perceived success of particular tactics, technologies, or organizational routines which serves as a guide to future learning efforts. In general, routines that have been successful will be used in the future, providing the opportunity for the group to further increase their expertise in that tactic or technology through continued use. Although this behavior can result in a group becoming specialized and expert in a given tactic or technology, this increasing aptitude can become a barrier to learning new technologies and techniques. Competency in a given technology can become a trap that blocks a group from pursuing new tactics or techniques.[41] If a new and an established technology are judged side by side based on

[38] Ortiz, R.D. “Insurgent Strategies in the Post-Cold War: The Case of the Revolutionary Armed Forces of Columbia.” *Studies in Conflict and Terrorism*, **25**:139, 2002

[39] Priest, D. and Farah, D. “Terror Alliance has U.S. Worried” *The Washington Post*, June 30, 2002, A1.

[40] Hoffman, B. Terrorist Targeting: Tactics, Trends, and Potentialities. RAND Report P-7801 (Santa Monica, CA: RAND Corporation, 1992) p. 9.

[41] Levitt, B. and March, J.G. “Organizational Learning” *Annual Review of Sociology*, **14**:322-3, 1988.

how successful they are, the new technology will always be handicapped by the group's lack of familiarity and skill in its use. Such competency traps can serve as a partial explanation of the observation that many terrorist groups have been operationally conservative and hesitant to adopt new tactics or weapons.[42] In the absence of compelling external reasons that change the apparent relative success of different attack forms, incentives work against displacing routines that are well established in an organization. Such competency traps can be reinforced if the organization has made substantial resource investments in a particular tactic or technique. In contrast, the variation in activities undertaken by al Qaeda – ranging from car bombings, maritime operations, and the attacks of September 11, 2001 – demonstrate that such traps do not affect all groups equally.

Although it seems self evident that an organization would guide its actions and future learning activities based on an assessment of the success of its current operations, actually putting such a rational process into practice can be quite difficult. In reality, it is often hard to impartially determine levels of organizational success or failure and even more difficult to tie changes in such a level of success with individual actions. Determining the success or failure of a particular action depends on an organization defining the outcomes it expects and then comparing what actually happens to those targets. Such an assessment could be particularly difficult for an activity like terrorism. In the example of suicide bombings included earlier, success was measured based on numbers of casualties. For attacks motivated by religious fundamentalism or a desire for revenge, this is likely an acceptable, if imperfect, metric. Conversely, if the overall goal of a group is to induce political change by carrying out attacks, it may be difficult to determine the absolute success of any given operation, much less compare the relative success of two operations using different tactics or weapons. In such campaigns, metrics based on numbers of causalities may be totally inappropriate. Success of an entire terrorist campaign might be recognizable – political recognition of the group's cause, obtaining an ethnic homeland, etc. – but the absolute success of any operation is not. Such a high level of ambiguity increases the potential for a group to reinterpret what

[42] A number of groups have been singled out for their reticence to change their modes of operations. They included the PLO, the PIRA, ETA, JRA, and the RAF. (Hoffman, B., Inside Terrorism, 197-198.)

constitutes success over time or to engage in "superstitious learning" where the relationships between actions and successful outcomes are drawn erroneously.[43]

Preserving Learning – Organizational Memory and Terrorist Group Structure

The key difference between organizational learning and individual learning by members of an organization is the encoding of experience in routines that can be passed on to other members of the group. Whether learning occurs incidentally through experience or *via* intentional research, the overall capabilities of an organization are not sustainably increased unless routines can pass from individuals into a collective organizational memory. This store of collective knowledge must be maintained over time and preserved by transfer to new group members through socialization. Depending on the characteristics of a group, an organizational memory could be maintained in systems of rules, standard operating procedures, training manuals or materials, common documents, usage of particular technologies, in addition to more abstract entities like group cultures and belief systems.

In the case of explicit knowledge, preservation of an organizational memory generally involves the archival collection of the relevant information, its preservation and maintenance, and structured transfer of the information to other group members. A example of such a collection of explicit knowledge is the multi-volume, 7000 page *Encyclopedia of the Afghan Jihad* assembled by al Qaeda.[44] Because tacit knowledge is often not easy to identify and capture, it is much more elusive than its explicit counterpart. As a result, sustainable organizational bodies of tacit knowledge are more difficult to construct. In fact, many organizations only realize that the tacit knowledge held by particular individuals is both critical and not "organizational" when those people leave the firm or group and the knowledge is lost. Methods to preserve tacit knowledge generally focus on structured training or interaction between organization members to promote information sharing. In addition, many organizations also devote considerable resources to capturing or recording tacit understandings as explicit knowledge in standard

[43] Levitt, B. and March, J.G. "Organizational Learning" *Annual Review of Sociology*, **14**:325-6, 1988.

operating procedures or other organization documents. Although this process can preserve tacit knowledge in a more enduring form, it is difficult and resource intensive.

Although capturing the results of individual learning activities into an organizational memory is potentially costly for any organization, knowledge management activities can have particular risks for terrorist groups. Because counterterrorist forces are constantly seeking information about terrorist organizations, any codified or explicit knowledge maintained by a group can represent a significant vulnerability. For example, the wealth of papers, videotapes, and notes discovered in various al Qaeda sites in Afghanistan have provided US intelligence with significant amounts of data on the group's members, operations, and plans.[45] As cited previously, the seizure of documents by police in a raid on the Italian group NAP also provided the authorities with significant amounts of information about the organization.[46] These risks are similar for other illegal organizations such as drug cartels.[47]

The risks posed by the maintenance of an explicit organizational memory once again underscore the importance of state sponsors or safe havens to the capacity of terrorist groups. In addition to providing venues for learning and sources of knowledge, sympathetic states can also provide a haven for group records and knowledge that might allow it to maintain a more complete and effective organizational memory. It is likely that one reason so many al Qaeda records and documents were found in Afghanistan[48] is because that nation had been a friendly haven to the group for a long period and its leaders believed that their adversaries would not be able to seize any organizational memory built there.[49] In general, however, one would expect the high level of

[44] Gunaratna, R. Inside Al Qaeda: Global Network of Terror (New York: Columbia University Press, 2002) 70.

[45] See, for example, Pincus, W. "Seized Materials May Help Thwart Future Attacks" *The Washington Post*, April 3, 2002, A14; http://www.cnn.com/SPECIALS/2002/terror.tapes (Last Accessed: Sept 8, 2002).

[46] Drake, R. The Revolutionary Mystique and Terrorism in Contemporary Italy. (Bloomington, ID: Indiana University Press, 1989) 30.

[47] Kenney, M. "When Criminals Out-smart the State: Understanding the Learning Capacity of Colombian Drug Cartels." *Transnational Organized Crime*, 5(1).

[48] Pincus, W. "Seized Materials May Help Thwart Future Attacks" *The Washington Post*, April 3, 2002, A14.

[49] In addition to the role of sympathetic states, terrorist group support communities may also play a role as knowledge repositories. They certainly play a role in hiding weapons and other supplies (explicit knowledge/technology).

uncertainty faced by terrorist groups would lead them to avoid codifying knowledge to the extent possible and to rely on more informally shared and tacit information.

Beyond the risks faced by terrorist groups from the potential compromise of their organizational memories, the effective construction and maintenance of such a group body of knowledge also requires effective mechanisms of knowledge transfer within the organization. If significant enough barriers exist to information transfer, learning will never be successfully embedded in routines shared by an entire group. Within commercial organizations, barriers to transfer of knowledge have been observed between separate units or divisions within a firm, even if the individuals involved freely and frequently interact. In many cases, firms have had to restructure or drastically modify their corporate cultures and practices to stimulate the transfer of technology and learning within the organization. Because of the particular pressures and structural forms adopted by terrorist groups, even more serious barriers to knowledge transfer might be expected.

In order to continue operating, a terrorist organization must protect itself from infiltration and compromise by law enforcement or intelligence personnel. This stringent requirement to prevent knowledge transfer outside the group has led most terrorist organizations to structure themselves in ways to both minimize the chances of such transfer and to reduce the potential damage if it does occur. The basic strategy adopted by most groups is to organize their activities based on a cell structure. A terrorist cell is a small group of individuals who operate together to plan and carry out attacks. The size of the group makes it possible for cell members to know each other well, thereby reducing the chances of infiltration. Depending on the size of the group, an overall terrorist organization will consist of one or more cells. For small groups, such as the Japanese Red Army or the Red Army Faction that had between 20 and 30 members,[50] the entire group might consist of a single cell. For larger organizations, the entire group will be made up of a number of individual cells. In order to reduce the risk to a larger organization, the group is compartmentalized – individual members may only know the identities of the others in their cell. Although this limits the damage if a cell is

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

compromised, this structure creates inherent barriers to information flow within the organization and handicaps learning for the group as a whole.

To further explore the impact of group structure on organizational learning, it is relevant to step through the range of structures adopted by terrorist groups. Although very small groups technically adopt a cellular structure, if the entire group belongs to one or two cells there are few barriers to intra-group communication and the maintenance of an organizational memory. Because the whole organization will interact regularly by necessity, knowledge will likely be readily shared.

For larger groups made up of many compartmentalized cells, the extent to which barriers exist to group learning will depend on whether routes of communication among cells exist. If group leaders or other individuals can serve as a bridge among different cells – through communication, direct interaction, or contact during the training of the cells – it may be possible for lessons learned by individual members or cells to be transferred to the larger organization. In this model, while most cell members are kept ignorant of the identity of other group members, a small number of individuals with broader knowledge of the group help offset the learning disadvantages of security. Evidence suggests that al Qaeda utilizes this approach where most members are kept ignorant of the identities of others but interaction between organizational leaders and intermediaries allows transfer of information and knowledge between cells.[51] Given the interest in terrorist use of the Internet, it is relevant to consider the role that information technology could also serve in reducing these information costs. If routes exist for anonymous communication between individual cells, it is possible for the exchange of explicit knowledge among groups that are otherwise ignorant of each others' identities.[52] In the absence of routes to allow interaction among cells of a larger group, it is debatable whether any organizational memory can be built. In such a situation, the individual cells

[51] Gunaratna, R. Inside Al Qaeda: Global Network of Terror (New York: Columbia University Press, 2002) 76-77.

[52] Although this would provide a way for tighter security on the personnel side – i.e. ensuring that no group member could compromise more than his or her own cell – it would open up groups to other cyber vulnerabilities. Such anonymous exchanges of information rely on a level of "blind trust" that the system has not been compromised and all participants are indeed group members.

might be best thought of as individual organizations with similar goals rather than elements of the larger terrorist groups.[53]

Beyond even multi-cellular organizations, an even more isolated and compartmented group structure is the strategy of “leaderless resistance” adopted over the past few years by certain terrorist groups. The basic principle of this strategy is that an individual or small group prepares publications (either physically or on the Internet) espousing their philosophies and suggesting targets that would be appropriate to advance their agenda. The intent of this behavior is that like-minded individuals will be persuaded to take the suggestion, act either individually or in small groups, and carry out the attacks. Examples of such groups include various radical right wing groups, militias, environmental and animal rights organizations, and violent anti-abortion activist groups. In some cases, the founders or core of the group give these individuals permission to claim their attack in the name of the overall terrorist organization. For example, guidelines on the Animal Liberation Front Internet site state: “Any group of people who are vegetarians or vegans and who carry out actions according to A.L.F. guidelines have the right to regard themselves as part of the A.L.F."[54] Although this leaderless resistance model is advantageous from the standpoint of security, it has very significant implications for organizational learning. Because the individual cells of these “groups” are completely unaware of the existence of each other and there is no contact between individual cells and any group leadership, there is virtually no route other than postings on the Internet or transmission in media reports for any knowledge to pass between group members. As a result, it is difficult to envision *any* route through which detailed, tacit knowledge gained by individuals in different pieces of the organization could ever be converted into enduring routines. This practical constraint could significantly limit the level of tactical advancement one would predict for “groups” which adopt this structure. In light of these observations, from an organizational learning perspective, it could be argued that organizations adopting the leaderless resistance model should not be

[53] In addition to learning difficulties, cellular structures can pose problems from the perspective of command and control. Cells may take actions that are not consistent with the overall goals of the group because the compartmentalization makes it difficult to exert authority over them and guide their actions. (See Jane’s Facility Security Handbook, June 1, 2000, Chapter I: Terrorism Primer)

[54] http://www.animalliberation.net (Last Accessed: Sept 17, 2002)

considered single groups but rather collections of similar but independently acting individuals.

Because of the significant pressures exerted on terrorist organizations by law enforcement and intelligence activities, such groups face particular challenges from the perspective of organizational learning. Efforts to capture and preserve knowledge, while helping to preserve group capabilities through turnover of individual members, could also compromise the group as a whole to its opponents. In addition, the structures adopted by terrorist group also can have a significant impact on their potential to learn at the organizational level. At one extreme, very small groups may be able to build organizational memories very effectively given the very high degree of interaction among their members. Large compartmented groups, on the other hand, put up intentional barriers to learning in the interests of preserving security. When focusing on the potential for terrorist groups to learn, they should most likely be viewed less as single organizations and more as collections of smaller groups, each with its own potential to learn and advance.

Concluding Remarks

In considering the problem of terrorism and the design of counter-terrorist strategies, an understanding of organizational learning can clearly be an important component in successful law enforcement or intelligence activity. Whether examining the learning that goes on around the highest strategic issues or at the most detailed tactical level, insight into how extremist groups change over time is critical for an understanding of how counter-terrorist approaches must change in response. Because of the impact of technology and tactics on the potential lethality of terrorist attacks, it is clear that the learning processes that make up technology adoption are of particular concern.

Although the processes described in this chapter do provide a picture of the relevant organizational learning activities of terrorist groups, it is important to point out that this analysis has focused almost entirely within the boundaries of single organizations. With the exception of drawing on outside individuals or groups as a source of knowledge, the processes have been described without reference to any influences outside the groups themselves. Like all other groups in social or economic systems, however, terrorist organizations do not operate in a vacuum. They are surrounded and interact with other groups engaged in learning processes of their own. Relevant examples include learning by the potential targets of terrorism that could reduce the efficacy of particular attacks or tactics, learning by the governments that terrorism is intended to influence in the ways they react to such violence, and learning by the counter-terrorist forces that are these groups direct adversaries. These interactions, the terrorist group's so-called "ecology of learning," can be a very significant influence or perturbation to the learning processes they undertake and the relative success of those efforts.

In fact, a major portion of counter-terrorism could be viewed as a learning contest between terrorist organizations and government groups. Intelligence and law enforcement organizations constantly seek protection solutions to defeat current attack methods, strategies to deter attacks at sites of particular concern, and to devise new ways to counter and apprehend the terrorists. Conversely, the terrorist groups seek new strategies to overcome countermeasures, better tactical information to support their attacks, and methods to elude capture. On a second level, both groups also struggle to influence the learning processes of their adversaries. Counter-terrorist forces attempt to disrupt terrorist learning through strategies such as misinformation campaigns, interfering with group intelligence gathering, prevention of training activities, elimination of safe havens, and counter-proliferation programs. At the same time, terrorist groups constantly seek to prevent intelligence and law enforcement from gathering the information about group activities needed for effective action. These adversarial relationships place terrorist organizations within a particularly competitive ecology of learning, one in which we all have a significant stake in the outcome of the competition. Comprehending these learning interactions and relationships is just as critical as understanding the processes within particular groups and represents an important area for future examination. Because of its direct attention to the complex interactions between the terrorist groups and their governmental or societal opponents, such a strategy may represent a unique opportunity for the field of organizational learning to suggest solutions to this critical problem in international affairs.