This product is part of the RAND Corporation monograph series. RAND monographs present major research findings that address the challenges facing the public and private sectors. All RAND monographs undergo rigorous peer review to ensure high standards for research quality and objectivity.

Sharing the Dragon's Teeth

Terrorist Groups and the Exchange of New Technologies

Kim Cragin, Peter Chalk, Sara A. Daly, Brian A. Jackson

Prepared for the Department of Homeland Security

RAND Homeland Security

A RAND INFRASTRUCTURE, SAFETY, AND ENVIRONMENT PROGRAM

This research was sponsored by the United States Department of Homeland Security and was conducted under the auspices of the Homeland Security Program within RAND Infrastructure, Safety, and Environment.

Library of Congress Cataloging-in-Publication Data

Sharing the dragon's teeth : terrorist groups and the exchange of new technologies / R. Kim Cragin ... [et al.].
p. cm.
"MG-485."
Includes bibliographical references.
ISBN 0-8330-3915-6 (pbk. : alk. paper)
1. Terrorism. 2. Terrorism—Technological innovations. I. Cragin, Kim. II. Rand Corporation.

HV6431.S46655 2007
363.325—dc22

2006012871

Published 2007 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Summary

Operation Enduring Freedom and the global war on terrorism forced many members of al Qaeda to disperse, as the U.S. government and its allies removed safe havens and arrested a number of key leaders.[1] As a result, the nature of the terrorist threat against the United States appears to have changed. For example, some like-minded terrorist groups that perhaps do not have the global reach of a pre-9/11 al Qaeda nevertheless have formed regional alliances. Similarly, other events have caused terrorist groups that are not linked ideologically to form mutually beneficial partnerships. These partnerships have provided otherwise less capable terrorist groups with the opportunity to improve their skills and their reach. In each circumstance, emerging alliances could increase the threat that terrorism will pose to the United States in the next 3–15 years. Understanding these interactions, therefore, is essential to ongoing and future efforts in the U.S. global war on terrorism.

Terrorist groups in three areas—Mindanao, the West Bank and Gaza Strip, and southwest Colombia—have exchanged technologies and knowledge in an effort to improve their operational capabilities. Studying these situations, therefore, can provide the Department of Homeland Security (DHS) with examples of why and how terrorists might share new technologies in the future, as well as the degree to which these exchanges might be successful. We chose these case studies because the terrorist groups active in these regions are highly capable.

[1] For example, Ramzi Binalshib and Abu Zubaydah in 2002, Khalid Sheikh Mohammad and Hambali in 2003, Ahmed Khalfan Ghailani in 2004, and Abu Faraj Farj al-Libbi in 2005.

Thus, the technologies and exchange processes are weighed toward *success* and should be of significant concern to the U.S. national security community.

This book examines a variety of different technologies and exchange processes, ranging from remote-detonation devices to converted field ordnance to *katyusha* rockets. In some instances, terrorists successfully obtained and deployed the technologies involved. Counterterrorism forces disrupted other technology exchanges.

- In Mindanao, Indonesian Jemaah Islamiyah (JI) trained and equipped Filippino militants. New technologies included remote-detonation technologies and improvised explosive devices (IEDs), as well as pressure-activated switches designed to detonate bombs, should security forces attempt to deactivate them. These exchanges improved the operational effectiveness and tempo of militant groups in the region from approximately 2003 to 2005.
- In the West Bank and Gaza Strip, Hizballah trained and equipped Palestinian militants. New technologies included IEDs and *katyusha* rockets, as well as suicide detonation devices. These exchanges provided militants with the ability to continue to escalate attacks against Israel from approximately 2000 to 2005.
- In southwest Colombia, the Provisional Irish Republican Army (PIRA) trained and equipped militants in the Revolutionary Armed Forces of Colombia (or FARC, for Fuerzas Armadas Revolucionarios de Colombia) in the former demilitarized zone. New technologies and knowledge included remote-detonation technologies and Mark 18 "barracks-buster" mortars, as well as guerrilla warfare tactics. These skills helped FARC improve its urban warfare capabilities in 2001.

In total, we examined 11 terrorist groups that operate in these three regions. Our research into each revealed vulnerabilities in technology exchanges between terrorist organizations, which led to eight overarching conclusions. These conclusions relate to (1) improving threat assessments, (2) disrupting innovation processes, and (3) affecting terrorist groups' cost-benefit analyses.

Improving Threat Assessments

Primarily, our research reemphasized the need for accurate, up-to-date threat assessments of terrorist groups. More importantly, our findings indicate that a threat assessment that ignores intergroup dynamics—including technology exchanges and beyond—is destined to be outdated quickly. These assessments would also benefit, according to our research, from a close examination of failed attacks. If terrorist groups attempt a particular tactic over and over again, this might represent an area in which they would invest in a new technology.

Similarly, the terrorist groups in our study weighed potential gains or costs in *operational capabilities* as more important than ideological similarities when choosing whether or not to participate in technology exchanges. For example, JI transferred technologies to like-minded Filipino militants, but in exchange derived *operational benefits* from access to safe havens in Mindanao. Hizballah similarly transferred knowledge to Palestinian militants through direct person-to-person contact, but only until Israeli counterterrorism forces began to arrest Hizballah's skilled trainers. It then shifted toward a more remote transfer of descriptive information of physical technology without instruction. This finding suggests that threat assessments should focus on operational as well as strategic motivations for alliances between terrorist groups.

Finally, analyses of individuals with technical knowledge tend to focus on chemical, biological, radiological, or nuclear (CBRN) technologies. While we do not want to detract from the importance of monitoring individuals with these technical skills, our findings suggest that analysts also should monitor individuals with technical expertise in remote-detonation technologies, rockets and missiles, IEDs, and converted field ordnances (mortars).

Disrupting Innovation Processes

We also discovered some factors that facilitated the exchange of technology between terrorist groups. In addressing these facilitating factors, the U.S. government should disrupt innovation processes and reduce

the potential for a successful exchange of technology. For example, in both Mindanao and southwest Colombia, terrorist groups transferred technologies most successfully through direct, person-to-person training. Terrorist groups could interact closely, because governments had provided them with *safe havens* as incentives for their participation in peace negotiations. Our findings question the utility of such an approach, especially if these safe havens are not monitored closely by third parties.

Additionally, the easy movement of people and goods across borders also facilitated the technology exchanges. In the cases of Hizballah and JI, these militant groups utilized existing smuggling routes to transport equipment and trainers. At least three PIRA members traveled from the United Kingdom to Colombia, without getting stopped by security officials. This suggests that tightening border security practices should also help disrupt technology exchanges between terrorist groups. In circumstances in which the U.S. government does not control borders yet is concerned about technology exchanges, it should consider providing appropriate training and equipment to these government authorities.

Finally, in the case of Hizballah and Palestinian militants, Israeli counterterrorism policies aimed at targeting individuals with technical skills served to disrupt advances in the groups' capabilities. In Chapter Six, we suggest that the U.S. intelligence community monitor the movement of individuals with technical skills, such as deploying remote-detonation devices, as well as CBRN weapon technology. We would also suggest that the U.S. government consider arresting these terrorists, should it become apparent that they are sharing knowledge across militant groups of concern to the United States. The U.S. government has already adopted this approach in certain areas, for example in Southeast Asia with its rewards program for JI militants in the Philippines. But, for the most part, U.S. programs focus on militants with links to al Qaeda. Our research suggests that these types of programs be expanded to include individuals with certain technical skills, in addition to leaders who have links to al Qaeda.

Affecting Terrorist Groups' Cost-Benefit Analyses

Our research indicates that the U.S. government would benefit from policies aimed at undermining the trust between terrorist organizations. In all three of our case studies, terrorists built on a foundation of trust when deciding to interact closely, as well as when these groups actually exchanged the technologies. To fracture this trust, U.S. policymakers could reveal suspicious leaks in groups' information security. Or, for cases in which money transfers occur, disrupt payment. These policies could help to exacerbate natural religious, political, or ethnic cleavages between these groups and create suspicion that individuals of the other group might turn trainers in to local authorities. With regard to other influence campaigns, U.S. security authorities might develop programs that attempt to change perceptions of a common enemy. Such policies would likely increase the costs associated with technology exchanges, reducing their potential for success.

Conclusion

DHS, in cooperation with other government agencies, is responsible for protecting the U.S. homeland against terrorist attacks. One way in which DHS can fulfill this responsibility is by anticipating and preparing for terrorist group innovations. Clearly, most innovations will take place beyond U.S. borders, but lessons learned could be applied to attacks inside the United States. Monitoring this flow of information and learning, therefore, is a key homeland security task. By examining how terrorist groups exchange technology and knowledge, this study provides DHS and other national security policymakers with some insight into the innovation process. It also suggests ways in which government policies can erect barriers to terrorists' adoption of new technologies.