NAVAL WAR COLLEGE
Newport, RI

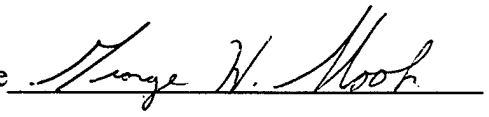
FORCE PROTECTION: THE PARANOID SURVIVE

by

George H. Slook
Lieutenant Commander, USN

A paper submitted to the faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my views and are not endorsed by the Naval War College or the Department of the Navy.

Signature 

5 February 2001

8

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED	
2. Security Classification Authority: NA	
3. Declassification/Downgrading Schedule: NA	
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.	
5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT	
6. Office Symbol: C	7. Address: NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207
8. Title (Include Security Classification): FORCE PROTECTION: THE PARANOID SURVIVE (U)	
9. Personal Authors: LCDR GEORGE H. SLOOK, USN	
10. Type of Report: FINAL	11. Date of Report: 5 FEBRUARY 2001
12. Page Count: 24	12A Paper Advisor (if any):
13. Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.	
14. Ten key words that relate to your paper: FORCE PROTECTION, ANTITERRORISM, TERRORISM, SECURITY, INTELLIGENCE SUPPORT, JOINT PLANNING, THEATER ENGAGEMENT	

15. Abstract: U.S. forces while engaged in commitments throughout the world in support of the National Military Strategy face a formidable threat from terrorists. This terrorist threat exists throughout the spectrum of military operations. Lessons from the past indicate that terrorists will seek to exploit weaknesses in our force protection. They will find seems in our woven force protection fabric and rip them open when we are least expecting. The U.S. military must not only learn from past incidents, but observe trends in terrorist organizations and closely monitor their capabilities to better provide force protection for its troops. Terrorist organizations are becoming increasingly global and are using technology to expand their reach, intelligence, targeting and lethality. As this threat evolves, so should our ability to counter that threat. The Geographic CINCs, Service Component Commanders and Joint Task Force commanders must lead a proactive approach in providing adequate force protection against this growing threat.

16. Distribution / Availability of Abstract:	Unclassified	Same As Rpt	DTIC Users
	X		
17. Abstract Security Classification: UNCLASSIFIED			
18. Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT			
19. Telephone: 841-6461		20. Office Symbol: C	

Security Classification of This Page Unclassified

Abstract

FORCE PROTECTION:

THE PARANOID SURVIVE

U.S. forces, while engaged in commitments throughout the world in support of the National Military Strategy, face a formidable threat from terrorists. This terrorist threat exists throughout the spectrum of military operations. Lessons from the past indicate that terrorists will seek to exploit weaknesses in our force protection. They will find seams in our woven force protection fabric and rip them open when we are least expecting them to do so.

The U.S. military must not only learn from past incidents, but observe trends in terrorist organizations and closely monitor their capabilities to better provide force protection for its troops. Terrorist organizations are becoming increasingly global and are using technology to expand their reach, intelligence, targeting and lethality. As this threat evolves, so should our ability to counter that threat.

The Geographic CINCs, Service Component Commanders and Joint Task Force Commanders must lead a comprehensive proactive approach to providing force protection against this growing terrorist threat. This approach should involve force protection planning throughout all phases of military operations. Without an antiterrorism element in our force protection planning, we will always be reacting to the terrorists' actions.

Introduction

In today's world, the main threat to many states, including specifically the U.S., no longer comes from other states. Instead, it comes from small groups and other organizations which are not states. Either we make the necessary changes and face them today, or what is commonly known as the modern world will lose all sense of security and will dwell in perpetual fear.[1]

Imagine the USS NIMITZ aircraft carrier, operating in the congested Arabian Gulf waters in the year 2005, as the target of a rocket propelled grenade attack that caused a flight deck conflagration resulting in 39 young sailors killed and the loss of half the topside aircraft. The delivery vehicle was a dhow that was transiting from Bandar-e 'Abbas, Iran to Bahrain. It looked just like any one of the hundred of dhows that made the same trip each day. The investigation report commissioned by the Secretary of Defense revealed that the crew did not recognize the dhow as being hostile, intelligence did not provide adequate warning of the attack, and the crew was not prepared to defend against a terrorist threat while on-station at sea. This scenario may sound far fetched, but so did the other major terrorist attacks on U.S. military forces prior to their occurrence.

Antiterrorism and force protection measures must be proactive vice reactive in order to become effective. The Geographic Combatant Commanders (CINCs), Service Component Commanders and Joint Task Force Commanders (JTFC) who are intimately familiar with the threats, plans and policies in their respective theaters must direct a comprehensive proactive approach to providing force protection against the terrorist threat.

While the terrorist organizations are changing their organizational structures, command and control media, and targeting and propaganda methods, there are some fundamentals that remain constant. Terrorists will seek to achieve their objectives by instilling fear throughout

their audience. Terrorists will instill fear through violence or the threat of violence. Additionally, they will seek to identify and exploit new vulnerabilities in force protection schemes to carry out their violence. Consequently, the U.S. military, while engaged throughout the range of military operations around the world, will face a formidable adversary. Whether conducting peacetime engagement activities or conducting war against a uniformed enemy, the threat from terrorists will be present. As this threat evolves, so should our ability to counter that threat.

This paper is organized in three parts. First, it will provide lessons learned from three past terrorist incidents against U.S. troops. It will show that following the attacks, measures were taken to prevent that incident from occurring again, but that the measures taken were limited in scope to the type of attack that precipitated that specific investigation. Each attack on U.S. troops shows that terrorists were able to exploit weaknesses in our force protection scheme that were previously considered secure. The second part of this paper will show how the terrorist threat is evolving and becoming more pervasive, lethal and persistent. The intent of this section is to demonstrate the need for the U.S. military to proactively develop antiterrorism/force protection (AT/FP) measures against growing terrorist capabilities. Due to the limited scope of this paper, this section will concentrate on the kinetic aspects of terrorism and not the growing non-kinetic aspects such as computer network attack. The third part of the paper will provide recommendations to the geographic Combatant Commanders, Service Component Commanders and Joint Task Force Commanders to better ensure force protection throughout the range of military operations.

Lessons From the Past

Beirut Bombing

On 29 September 1982, U.S. military forces entered Lebanon as part of a Multinational Force composed of U.S., French, Italian and British forces. The mission for the U.S. Marines was to establish conditions that would permit the withdrawal of foreign military forces from Lebanon and to assist the Lebanese government and armed forces in establishing control throughout the Beirut area. Initially, the environment was benign, but deteriorated rapidly in April 1983 with the destruction of the U.S. Embassy in Beirut. Following the embassy bombing, the U.S. Marines were the targets of car bombings, sniper attacks, and mortar attacks. Between May and November 1983, Marines received over 100 intelligence reports warning of possible terrorist car bomb attacks. On 23 October 1983, a large truck laden with the equivalent of over 12,000 pounds of TNT crashed through the perimeter of the U. S. Marine compound at Beirut International Airport, penetrated the Battalion Headquarters building and detonated. The explosion killed 241 U.S. Marines.[2]

The Department of Defense Commission convened by the Secretary of Defense to conduct the investigation into the bombing came up with the following conclusions: 1) The Marine Commander was not provided with timely intelligence, tailored to his specific operational needs, that was necessary to defend against the entire spectrum of threats he faced. 2) The security level was not commensurate with the level of the threat. 3) The U.S. Marines were not trained, organized, staffed, or supported to effectively defend against the terrorist threat in Lebanon. The Commission made the following recommendations to the Secretary of Defense: 1) Establish an all-source fusion center that would tailor all-source intelligence, with improved HUMINT support, to U.S. military commanders involved in military operations in areas of high threat, conflict or crisis. 2) Develop doctrine, planning,

organization, force structure, education and training sufficient to defend against terrorist attacks.[3]

Khobar Towers Bombing

During the night of 25 June 1996, a sewage truck filled with over 20,000 pounds of TNT parked on a road along the north perimeter fence of Khobar Towers, Dhahran, Saudi Arabia, a housing compound used by U.S. and Allied forces supporting Operation SOUTHERN WATCH. The truck drivers fled the scene and four minutes later the truck exploded. The explosion killed 19 U.S. military personnel and wounded over 500 persons.[4]

Unlike the situation in Beirut, the military personnel in Dhahran were over 175 miles away from the declared hostile zone. Besides the bombing of the Office of the Program Manager, Saudi Arabian National Guard (OPM-SANG) Headquarters in Riyahd in Nov 95, there had only been one other terrorist incident in the Kingdom. Additionally, the housing compound was heavily fortified with a perimeter fence and Saudi police providing 24 hour random patrol coverage outside the perimeter. U.S forces were responsible for security inside the compound utilizing area patrols and rooftop sentries.[5]

The Downing Report, containing an investigation into the security at U.S. military bases in the CENTCOM AOR following the Khobar Towers bombing, identified 26 findings. This report called for: 1) a greater flow of intelligence from the CINC to lower echelons in the chain of command; 2) a vulnerability assessment of U.S. facilities in the region; 3) a recommendation to relocate facilities to secluded areas when possible; 4) employment of integrated technology systems to detect, delay or mitigate the terrorist threat; and 5) the establishment of threat based stand-off or exclusion areas around compounds and bases. As in the Long Commission Report, the chain of command was found to have been inadequate in providing guidance and support to the Wing Commander at Dhahran.[6]

Following this incident, the U.S. made great efforts to increase security in the CENTCOM AOR. Security at fixed installations in CENTCOM's AOR and throughout the world was drastically increased. The Joint Chiefs of Staff produced Joint Publication 3-07.2 to better delineate responsibilities, tactics, techniques and procedures for antiterrorism. Independent contractors were hired to assess vulnerabilities and provide security solutions at major fixed military installations. While significant improvements were made to fixed installations, very little was done to protect those forces conducting engagement activities that were not attached to fixed installations.

USS COLE Bombing

On 12 October 2000, the USS COLE (DDG 67), while making a brief stop for fuel at Aden, Yemen, was attacked by two suicide terrorists in a boat loaded with explosives. Seventeen sailors were killed and 38 were injured. The cost of repair has been estimated to be 240 million dollars U.S.[7]

The USS COLE was steaming independently through the Suez Canal to join the Abraham Lincoln Battle Group in the Northern Arabian Gulf. The Commander, U. S. Naval Forces Central Command, based his decision to plan and approve the fuel stop at Aden on two issues: 1) the need to further the CINC's theater engagement strategy for Yemen and 2) a deterioration of security at the Navy's traditional fuel stop, Djibouti. Central Command assessed Yemen's threat level to be lower than that of Djibouti.[8]

Unlike the delivery method in the first two cases, these terrorists used a small boat. However, similar to the other incidents, the delivery vehicle blended in with the surrounding environment. Sailors interviewed believed it was simply another service craft. Commander USNAVCENT stated that the "battlefield" scene was devoid of both hostile act and hostile intent.[9]

The USS COLE Commission, directed by the Secretary of Defense following the bombing, found that a significant weakness in force protection existed with in-transit units. The term in-transit applies to both "inter" and "intra" theater. The report stated that both the CINC and Service Component Commanders are critical in establishing a balance between the benefits and risks associated with overseas theater engagement. It was their finding that the Component Commander, with the war-fighting mindset for the region, and ability to control resources has the responsibility to tailor specific AT/FP measures to protect transiting units. Specifically, the commission recommended that: (1) The U.S. Military CINCs and Service Component Commanders must become more proactive in applying AT/FP techniques and assets to enhance the AT/FP and deterrence posture against terrorists. (2) The U.S. must reprioritize resources for collection and analysis, including human intelligence (HUMINT) and signal intelligence (SIGINT) against terrorism. This intelligence must be tailored for in-transit units to combat the terrorist threat in their immediate area of operation. (3) Pre-deployment AT/FP training must be expanded to include AT/FP measures specific to the area of operation and accomplished to the same extent as a primary mission area. (4) The Geographic CINC shall have the sole authority for assigning the threat level for a country within his area of responsibility.[10] In effect, the report stated that the Geographic CINC, through his Service Component Commanders, is responsible for coordinating between Department of Defense (DoD), Department of State (DoS) and other agencies to ensure that transiting units have adequate intelligence, training and equipment tailored to defend against the terrorist threat.

Future Challenges We Will Face From the Terrorist Threat

The threat from terrorism that U.S. forces currently face has evolved tremendously over the last ten years and will continue to evolve throughout this decade. Terrorist organizations are rapidly integrating technology to increase their reach, targeting, lethality and effectiveness. [11] Terrorist organizations are becoming more transnational and are developing a global reach that can affect U.S. forces anywhere and throughout the range of military operations. Their goals are shifting from local political issues to broader religious and ideological goals, often resulting in a more fanatical approach.[12] Additionally, terrorist organizations are relying less on state sponsorship and more on non-state sponsorship, making them less susceptible to U.S. and world diplomatic and economic pressure.[13] The net result is that U.S. forces will be facing a much more formidable terrorist threat throughout the spectrum of military operations.

The Changing Face of Terrorism

The trend in the 1990s has been toward non-state sponsorship of terrorism. Our national strategy of imposing political, diplomatic and economic sanctions on countries sponsoring terrorist groups has proven fairly successful against state-sponsored groups. However, with the decrease of state funding, many organizations have developed their own sponsorship through private bank accounts, donations, illegal trade, narcotics trafficking and legitimate businesses. Increased sanctions forced upon terrorist organizations by states have prompted groups to take residence in states unwilling or incapable of taking such measures.[14] The CIA document, Global Trends 2015, predicts that non-state organizations will continue to expand and will become one of the top threats to our national security.[15]

Afghanistan is a country that is increasingly becoming a safe haven for terrorists. Osama bin Laden, leader of al-Qaida set up residence in Afghanistan after being ousted from Saudi Arabia. The Taliban in Afghanistan has been unwilling to take action against Osama bin Laden, despite US and UN sanctions, a United Nations Security Council resolution, and other international pressure.[16] Therefore, he has been free to use Afghanistan as a training ground and base of operations. Other terrorist groups have migrated to countries that are either unwilling to or incapable of extraditing terrorist groups.[17] These new non-state sponsored terrorist groups are less susceptible to the traditional political and economic sanctions that have been used effectively against state-sponsored groups.[18]

Another trend that poses a significant challenge to the U.S. is that terrorist organizations are becoming transnational. These new organizations tend to be more loosely organized cells or groups that are part of international networks. Their hierarchy tends to be much flatter enabling them to act independently with greater speed and enabling them to "swarm" or mass effects.[19] The gathering, from around the world, of protesters in Seattle for the 1999 World Trade Organization summit clearly demonstrated a "swarming" ability of very loosely networked groups with independent purposes, but with the single overarching goal of opposing globalization.[20] Following the summit, the protestors immediately dispersed throughout the world.

Osama bin Laden's al Qaida organization is an excellent example of a transnational network that is comprised primarily of relatively autonomous groups including many Sunni Islamic extremist groups such as factions of the Egyptian Islamic Jihad, the Gama'at al-Islamiyya, and the Harakat ul-Mujahidin.[21] These groups have local objectives but collectively have a global goal in opposing threats to Islam.[22] The groups are trained by Bin

Laden's organization, but then disperse throughout the region or world and act semi-autonomously to accomplish a common overarching goal. In 1992, Osama bin Laden's al Qaida organization set up a cell in Kenya, using legitimate businesses, to conduct operations in neighboring Somalia. Investigations indicate that in 1998, this same terrorist cell bombed the American Embassy in Kenya. A key point here is that this transnational terrorist group crossed no international borders to conduct devastating damage a continent away from their home base of operations. The challenge these loosely organized transnational groups present is that they significantly hamper our ability to predict their actions and monitor their activities. Groups can strike us throughout the world with little or no warning.[23]

In addition to training fighters in Somalia, al Qaida has sent cells to Bosnia and Chechnya as well as training fighters from the Philippines and Pakistan.[24] This is significant since it indicates that a terrorist organization is capable and willing to use local conflicts to achieve their more global overarching goals. The challenge this presents is that the U.S. military will be facing an additional adversary when engaged in operations throughout the world.

Another trend that will present significant challenges to us is that these new transnational organizations are emerging with religious or ideological goals that oppose our interests. The number of recognized religious terrorist groups increased from 16 in 1994 to 26 in 1995.[25] In 1995, Secretary of State, Madeleine Albright produced a list demonstrating that over half of the world's 30 most dangerous terrorist groups were based on religious beliefs including Judaism, Islam and Buddhism. These religious or ideological groups tend to be much more fanatical than in the past and tend to have much longer time lines for accomplishing their goals.[26]

Osama bin Laden very explicitly stated that his al Qaida is waging a *Jihad*, or holy war against US citizens and military throughout the world in order to "reestablish the Muslim state".[27] In 1998, in an attempt to further unite Islamic extremist groups, he called on all Muslims to kill Americans, including civilians, anywhere possible. While he may not have legitimate authority in the Muslim world to declare a Jihad, this still presents a tremendous challenge for us since it means we will be facing a global threat with the common goal of ejecting American influence throughout Islam. Their current means of achieving this goal is through inflicting heavy casualties on U.S. personnel worldwide. The implication for the military planner is that we will now always be fighting an enemy throughout the range of military operations. The enemy we will face will not simply be fighting to achieve short-term local objectives, but will have a long-term, broad objective of reducing U.S. influence. However, we will not always be able to identify that enemy by uniform alone. We will not be able to focus solely on the uniformed conventional threat, but will have to consider the non-uniformed threat fighting asymmetrically with unconventional methods. This will not be a trivial matter.

The Role of Technology

The reliance on modern high-speed communications has changed the way terrorist groups are organized and controlled. These new loosely organized transnational terrorist groups are becoming increasingly dependent on the internet to recruit members, obtain funds, coordinate activities and spread propaganda and ideology. Their hierarchy is becoming much flatter, resulting in greater speed of movement. Organizational leaders are able to provide strategic guidance to dispersed, tactically independent cells while monitoring their actions.[28] Ironically, the World Wide Web was the primary method used to bring the anti-globalization demonstrators together during the World Trade Organization summit meeting in Seattle.

Organizations are relying more heavily on satellite phones with encryption devices as well as developing secure methods of internet usage as command and control mediums.[29]

In addition to using modern high-speed communication means for directing operations, terrorist groups may increasingly use these media for spreading propaganda and gaining support. Groups such as Hizbullah, which manages three World Wide Web pages, make extensive use of the internet for spreading propaganda.[30] Media exposure will continue to play a significant role in terrorist targeting. The implication for the U.S. is that in order to continue to ensure media attention, the terrorist attacks must become more dramatic and/or destructive.[31] Attacks must be conducted against targets that will garner maximum coverage, i.e. the US military, as in the Beirut, Khobar Towers and USS Cole bombings. These bastions of US military might were previously thought of as invulnerable to attack. Attacks designed to produce large numbers of casualties as in the World Trade Center and Oklahoma City federal building bombings produced extensive world-wide media coverage. Terrorist organizations will tread the fine line between instilling mass fear and isolating themselves from their allies. When Timothy McVeigh was asked by his attorney if he could have achieved the same effect without the killing, he stated: "That would not have gotten the point across. We needed a body count to make our point."[32]

Lethality of weapons has greatly increased and will continue to increase with the proliferation of weapons of mass destruction (WMD). In 1983, the bomb used against the Marine barracks in Beirut consisted of 12,000 pounds of high explosives.[33] At the time it was described as the "largest non-nuclear blast ever detonated on the face of the earth."[34] In 1996, the Khobar Towers bomb became the largest to date estimated at 20,000 pounds of TNT equivalent.[35]

To date, terrorist use of WMD has been limited to the Aum Shinrikyo group's use of the sarin nerve agent in 1995. Global Trends 2015 states that the potential for unconventional delivery of WMD by non-state actors, such as terrorist groups, is likely to grow significantly in the next ten years.[36] Additionally, some terrorist groups, including Osama Bin Ladin's al Qaida, have publicly declared that they are attempting to acquire chemical, biological, radiological and nuclear weapons (CBRN). Regardless of the veracity of their proclamation, the CBRN materials, information and technology have become more widely available from the internet and from the former Soviet Union.[37]

Radiological weapons may bridge the gap between WMD and conventional weapons. Terrorists first used these weapons in 1995 when Chechen separatists buried thirty-five pounds of Cessium-137 in a Moscow park. Although testing by Russian officials determined that the material posed no serious health threat, it demonstrated the ability of a terrorist group to use radioactive material to instill general fear.[38] These radiological weapons are designed to disperse radioactive material over an area by either mechanical means or ordinary explosive, but do not require weapons grade material or a complicated delivery vehicle. Additionally, terrorists have the capability to "grind up" radioactive material for use in an air dispersal by any type air vehicle, including remotely controlled planes with wingspans as small as nine feet. The material could also be placed in ventilation systems or water reservoirs. The abundance of nuclear material combined with the ease of delivery through inexpensive unconventional means make this a highly likely weapon for future terrorist attacks.[39]

Another challenge we will have to confront is that terrorists will have greater access to high technology intelligence gathering and targeting systems. Commercial satellite imagery

is now easily obtainable. Terrorist organizations will be able to obtain vast amounts of information through the internet, world news organizations, accessible databases and through collaboration and networking. Hand held GPS systems are inexpensive, available and accurate. Accurate targeting combined with the proliferation of inexpensive delivery vehicles open up entirely new methods of attack for terrorists.

Many argue that despite the proliferation of inexpensive high tech devices, many terrorist organizations will continue to use what has worked for years: the gun and the bomb. While this may remain true for traditional terrorist groups with local interests, the new transnational groups seeking global media coverage will seek new and more destructive methods to attack. The characteristic of terrorist attacks that will likely remain is that the delivery vehicle for the weapon will most likely remain unconventional. As in previous attacks, it will blend in with the environment and exhibit no hostile intent to its intended victims.

Recommendations

Force protection must become a fundamental element in all phases of military operations. Whether the operation consists of a single unit accomplishing the Geographic CINC's theater engagement plan or a Joint Task Force (JTF), operational planning must take into account: 1) intelligence gathering, analysis, and dissemination, 2) force structure for security and 3) effective force protection measures. The JTF Commander must establish a FP cell, whose focus includes antiterrorism, prior to the start of the planning process and maintain it throughout the operation. Geographic CINCs through their Service Component Commanders must also establish FP operation cells within their staffs to cover all military

forces within their AOR not attached to a JTF. Additionally, a separate intelligence cell should be established with a focus on AP/FP.

Intelligence

> *What is called 'foreknowledge cannot be elicited from spirits, not from gods, nor by analogy with past events, nor from calculations. It must be obtained from men who know the enemy situation.*[40] *Sun Tzu*

The Geographic CINCs, Service Component Commanders and JTF Commanders must establish a FP intelligence cell that focuses on gathering and analyzing all-source intelligence including human intelligence (HUMINT) and signal intelligence (SIGINT) in areas of AT/FP. The FP intelligence cell must provide an intelligence preparation of the battle space (IPB) with regard to the terrorist threat. Geographic CINCs must be able to use this intelligence to determine the threat conditions (THREATCONs) throughout the joint operations area. Additionally, the military planners must be able to use this intelligence to determine which forces to employ and where to deploy them to maximize FP while accomplishing the mission. In the employment phase, the FP intelligence cell must be able to disseminate timely, analyzed intelligence that provides indications and warning of attack throughout the units of the JTF or AOR. Additionally, the AT/FP intelligence cell should provide daily updates so planners adequately incorporate AT/FP into branches and sequels.

Force Structure

During the planning phase, the FP operations cell must use the IPB to determine the AT/FP tasks and identify deficiencies in force structure and capabilities. The FP operations cell needs identify the joint forces required to provide adequate AT/FP throughout the range of operations and have an input into the TPFDD process. The cell's scope should include staging, and refueling bases that are within the combat and communication zones or AOR for

Geographic CINCs. Often, this will require liaison with other agencies including the Department of State to ensure foreign security forces are adequately equipped and trained. Service Component Command FP operation cells must identify force protection tasks to deploying commands to ensure that they are adequately equipped and trained with the correct mix of lethal and non-lethal weapons to counter the terrorist threat.

Force Protection Measures

The FP operation cells must constantly assess and evaluate the force protection measures against the increasing capabilities of terrorist groups. Sufficient forethought and anticipation must be given, based on analyzed intelligence and projections, so that capabilities and procedures are in place and have been rehearsed prior to terrorists having achieved sufficient capability to strike. These measures must be tailored to each specific operation so that deploying units will be able to implement them within their capabilities and rules of engagement. An additional task for the CINC/Service Component Command FP cells would be to determine if AT/FP measures are sufficient prior to a unit conducting any theater engagement. The cell will then serve as a pre-positioned liaison between the host nation and the participating unit.

Conclusion

We will never be able to ensure complete security of our forces against the terrorist threat. The terrorist threat will exist throughout the range of military operations. Lessons from the past indicate that terrorists will always seek to exploit weaknesses in our force protection. They will find these seams in our woven fabric with which we protect ourselves and rip it open when we are least prepared. Each time they have "successfully" attacked, the U.S. has conducted investigations to verify that they have indeed attacked our seams, and then we make recommendations to shore up our force protection measures. Changes are

made and doctrine written and revised to prevent similar situations from occurring again. To this extent we have been successful, since terrorists have rarely attacked in the same exact way twice.

Our AT/FP policy, however, must become more proactive vice reactive in order to become truly effective. The Geographic CINCs, Service Component Commanders and Joint Task Force Commanders must direct the more proactive approach by incorporating AT/FP intelligence and planning cells throughout all phases of operations. They must establish intelligence capabilities to detect terrorist trends and projected capabilities to enable deploying units to be adequately prepared to meet their expected threats. They must ensure that tailored, analyzed intelligence on the terrorist threat is provided to the operational commander so that he can incorporate force protection planning throughout the spectrum of military operations. Lastly, CINCs must evaluate their theater engagement plans to ensure that the risks of execution do not outweigh the benefits.

Terrorists' capabilities and methods of attack and organizational structure are constantly evolving. Terrorist organizations in the future will capitalize on the proliferation of inexpensive, available technology to enhance command and control, intelligence, targeting, effects and exposure. Despite the many uncertainties surrounding where, who, how and when terrorists will attack, there are also many certainties. These certainties are that terrorists will continue to attack our vulnerabilities with unconventional means. They will attempt to achieve mass casualties, to seek maximum exposure, and to instill fear throughout their target audience and the world at large.

NOTES

[1] Martine Van Creveld, quoted in Ian O. Lesser and others, Countering the New Terrorism, (Santa Monica: The Rand Corporation, 1999), 42-43.

[2] Robert L. J. Long, Report of the DoD Commission on Beirut International Airport Terrorist Act, October 23, 1983, (Washington: DC: 1983), 1-3.

[3] Ibid., 9-15.

[4] Douglas R. Cochran, "Force Protection Doctrine: An Operational Necessity," (Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1998), 1.

[5] Ibid., 6-8.

[6] Wayne A. Downing, Force Protection Assessment of USCENTCOM AOR and Khobar. Towers, (Washington: August 30,1997), xiv-xviii.

[7] "Navy Announces Results of its Investigation on USS Cole (DDG 67)," U.S. Department of the Navy, 19 January 2001, <http://www.chinfo.navy.mil/navpalib/news/newsstories/cole.html>, [26 January2001], 2-4.

[8] "First Endorsement to Investigating Officer's Report," SECNAV/CNO Reading Room-USSCOLE, January 2001, <http://www.foia.navy.mil/USSCOLE/> [25 January 2001], 122-124.

[9] Ibid., 129.

[10] U.S. Department of Defense, DoD USS COLE Commission Report, 9 January 2001, <http://www.defenselink.mil/pubs/cole20010109.html>, [13 January 2001], 1-8.

[11] Ian O. Lesser and others, Countering the New Terrorism, (Santa Monica: The Rand Corporation, 1999), 43.

[12] Ibid., 15-19.

[13] Ibid., 107.

[14] U.S. Department of State, Patterns of Global Terrorism 1999, (April 2000), iii.

[15] "Global Trends 2015: A Dialogue About the Future With Nongovernmental Experts,"

National Intelligence Council 2000-02, December 2000, <http://www.cia.gov/cia/publications/globaltrends2015/index.html>, [2 January 2001], 8.

[16] Ibid., 7.

[17] Ibid.

[18] Ibid., 107-108.

[19] John Arquilla, David Ronfeldt and Michele Zanini, "Terrorism in the Information Age," Current History, (April 2000): 181.

[20] Wayne Hall, "The Janus Paradox: The Army's Preparation For Conflicts of the 21st Century," n.p.: n.p., (August 2000): 17.

[21] U.S. Department of State, Global Terrorism, 85.

[22] Arquilla, Ronfeldt and Zanini, 184

[23] "Regional Threats to U.S. Interests and Security," United Sates Central Command, December 2000, <http://www.centcom.mil/theater_strat/regional_threats.htm> [29 December 2000], 3.

[24] U.S. Department of State, Global Terrorism, 31.

[25] Mark Juergensmeyer, "Understanding the New Terrorism," Current History, (April 2000): 158.

[26] Ibid.

[27] U.S. Department of State, Global Terrorism, 84.

[28] Arquilla, Ronfeldt and Zanini, 183.

[29] Ibid., 184.

[30] Juergensmeyer, 66.

[31] Ian O. Lesser and others, 12-13.

[32] Ibid., 13.

[33] Long, 3.

[34] Eric Hammel, quoted in Lesser and others, Countering the New Terrorism, (Santa Monica: The Rand Corporation, 1999), 15.

[35] Douglas R. Cochran, 7.

[36] "Global Trends 2015," 9.

[37] U.S. Department of State, Global Terrorism, 36.

[38] Matthew E Woods, "The Threat of Radiological Terrorism," Defense Technical Information Center, (April 1997): 62.

[39] Ibid., 76.

[40] Samuel B. Griffith, Sun Tzu The Art of War, (Oxford, England: Oxford University Press 1971), 145.

BIBLIOGRAPHY

Arquilla, John., David Ronfeldt and Michele Zanini. "Terrorism in the Information Age," Current History, (April 2000): 179-187.

Center For Naval Analysis. Naval Studies Group. Future Uses of Non-lethal Weapons. Alexandria, VA: 2000.

Cochran, Douglas R. "Force Protection Doctrine: An Operational Necessity." Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1998.

Cohen, William, S. "Security in a Grave New World." Speech. Council on Foreign Relations, New York, NY: 14 September 1998. Lkd. Office of Assistant Secretary of Defense at "Defense Link Page." <http://www.defense link.mil/cgi-bin/dlprint.cgi> [29 December 2000].

Downing, Wayne A. Force Protection Assessment of USCENTCOM AOR and Khobar. Towers. Washington: August 30, 1997.

"Global Trends 2015: A Dialogue About the Future With Nongovernmental Experts." National Intelligence Council 2000-02. December 2000. http://www.cia.gov/cia/publications/globaltrends2015/index.html [2 January 2001]

Griffith, Samuel B. Sun Tzu The Art of War. Oxford, England: Oxford University Press 1971.

Hall, Wayne, M. "The Janus Paradox: The Army's Preparation For Conflicts of the 21st Century," n.p.: n.p. 4 August 2000.

Hanley, James N. "Force Protection of Strategic Airlift Forces in the Operations Other Than War Environment." The IDTC Review, 3 (March 1997):

"Investigating Officer's Report." SECNAV/CNO Reading Room-USS COLE. January 2001. <http://www.foia.navy.mil/USSCOLE/> [25 January 2001].

Jenkins, Robert Michael. The Lessons of Beirut: Testimony Before the Long Commission. Santa Monica, CA: The Rand Corporation, 1984.

Juergensmeyer, Mark. "Understanding the New Terrorism." Current History, (April 2000): 158-163.

Kozaryn, Linda D. "Cohen Touts Force Protection Via Wordwide Video-call." American Forces Information Service News Articles. 27 October 2000. <http//www.defense Link.mil/news/Oct2000/n10272000_200010272.html> [10 January 2001]

Kugler, Richard, L. Changes Ahead: Future Directions for the U.S. Overseas Military Presence. Santa Monica, CA: The Rand Corporation, 1998.

Lesser, Ian, O., Bruce Hoffman, John Arquilla, David Ronfeldt, Michele Zanini, Countering the New Terrorism. Santa Monica: The Rand Corporation, 1999.

Long, Robert L.J., Admiral, USN (Retired). Report of the DoD Commission on Beirut International Airport Terrorist Act, October 23, 1983. Washington: December 20, 1983.

National Commission on Terrorism. Countering the Changing Threat of International Terrorism. Washington, DC: 1999.

"Navy Announces Results of its Investigation on USS Cole (DDG 67)." U.S. Department of the Navy. 19 January 2001. <http://www.chinfo.navy.mil/navpalib/news/news_stories/cole.html>[26 January2001]

"Regional Threats to U.S. Interests and Security." United Sates Central Command. December 2000. <http://www.centcom.mil/theater_strat/regional _threats.htm> [29 December 2000].

"Second Endorsement to Investigating Officer's Report." SECNAV/CNO Reading Room-USSCOLE. January 2001. <http://www.foia.navy.mil/USSCOLE/> [25 January 2001].

Smedberg, William R. "The Battle Fleet Must Have Eyes." Proceedings, (September 1998): 89-90.

"Third Endorsement to Investigating Officer's Report." SECNAV/CNO Reading Room-USS COLE. January 2001. <http://www.foia.navy.mil/USSCOLE/> [25 January 2001].

"Training and Equipment Requirements." USCINCENT OPORD 97-01A, November 1999. <http://www.centcom.smil.mil/ccjs/jsd_areas/deployments/equipment.htm> [12 January 2001].

"U.S. Counterterrorism Efforts Since the 1998 U.S. Embassy Bombing in Africa." Department of State Fact Sheet. 7 August 2000. <http://www.state.gov/www/global/terrorism/fs_000807_counterterror.html> [29 December 2000].

U.S. Department of Defense. DoD Combating Terrorism (DoD Directive 2000.12) Washington, DC: September 15, 1996.

U.S. Department of Defense. DoD USS COLE Commission Report. 9 January 2001. <http://www.defenselink.mil/pubs/cole20010109.html> [13 January 2001].

U.S. Department of State. Patterns of Global Terrorism 1999. April 2000.

U.S. Joint Chiefs of Staff. Doctrine for Intelligence Support to Joint Operations. Joint Pub. 2-0. Washington, DC: 2000.

U.S. Joint Chiefs of Staff. Doctrine for Joint Military Operations Other Than War. Joint Pub. 3-07. Washington, DC: 1995.

U.S. Joint Chiefs of Staff. Doctrine for Joint Operations. Joint Pub. 3-0. Washington, DC: 1995.

U.S. Joint Chiefs of Staff. Doctrine for Planning Joint Operations. Joint Pub. 5-0. Washington, DC: 1995.

U.S. Joint Chiefs of Staff. Interagency Coordination During Joint Operations, Vol. II. Joint Pub. 3-08. Washington, DC: 1996.

U.S. Joint Chiefs of Staff. Joint Tactics, Techniques, and Procedures for Peace Operations. Joint Pub. 3-07.3. Washington, DC: 1999.

U.S. Joint Chiefs of Staff. Joint Tactics, Techniques, and Procedures for Antiterrorism. Joint Pub. 3-07.2. Washington, DC: 1998.

U.S. Joint Chiefs of Staff. National Military Strategy of the United States of America. Washington, DC: September 1997.

U.S. President. A National Security Strategy for a New Century. Washington, DC: The White House, December 1999.

Woods, Matthew E. "The Threat of Radiological Terrorism." Defense Technical Information Center (April 1997)