REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
09-02-2004	FINAL	

4. TITLE AND SUBTITLE

The Next Terrorist Attack: Not If, But When…Are We Prepared?

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

David F. Lynch, Major, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES 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. ABSTRACT Senior leaders continually warn of future terrorist attacks and acknowledge the United States will not be able to prevent all attempts. Consequently, National Strategies highlight the importance of preparing responses for when prevention fails. Since lessons learned from past attacks call attention to the terrorist's ability to overcome military defenses, the importance of well-developed, exercised response plans cannot be overstated. Department of Defense directives charge the combatant commanders with developing those responses to protect U.S. Forces. Although, while commanders spend billions of dollars building stronger defenses, Joint Staff assessment teams continue to find response plans do not exist, are not coordinated with responsible agencies or not exercised.

The combatant commander must find a method to break the "bunker mentality" and move beyond a solely defensive antiterrorism strategy. By translating national strategy through campaign planning and applying the essence of operational art, the combatant commander will increase the efficacy of his antiterrorism program. Viewed as a series of major operations divided into three phases (prevention, response, and continual improvement), the theater antiterrorism campaign will move subordinate commanders beyond their defense-centric strategy. Establishing adequate physical security standards, transitioning through each campaign phase, prioritizing command installations and integrating existing plans are key elements of the campaign plan. Only when combatant commanders have well-developed--and exercised--response plans will U.S. Forces truly be prepared for the next terrorist attack.

15. SUBJECT TERMS
Terrorism, response plans, antiterrorism campaign, antiterrorism plan, consequence management

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
					Chairman, JMO Dept
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER *(include area code)*
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		26	401-841-3556

Standard Form 298 (Rev. 8-98)

NAVAL WAR COLLEGE
Newport, R.I.

The Next Terrorist Attack: Not If, But When…Are We Prepared?

By

David F. Lynch
Major USAF

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 own personal views and are not necessarily endorsed by the Naval War College, Department of the Navy or the Department of the Air Force.

Signature: _____
9 Feb 04

TABLE OF CONTENTS

ABSTRACT

Senior leaders continually warn of future terrorist attacks and acknowledge the United States will not be able to prevent all attempts. Consequently, National Strategies highlight the importance of preparing responses for when prevention fails. Since lessons learned from past attacks call attention to the terrorist's ability to overcome military defenses, the importance of well-developed, exercised response plans cannot be overstated. Department of Defense directives charge the combatant commanders with developing those responses to protect U.S. Forces. Although, while commanders spend billions of dollars building stronger defenses, Joint Staff assessment teams continue to find response plans do not exist, are not coordinated with responsible agencies or not exercised.

The combatant commander must find a method to break the "bunker mentality" and move beyond a solely defensive antiterrorism strategy. By translating national strategy through campaign planning and applying the essence of operational art, the combatant commander will increase the efficacy of his antiterrorism program. Viewed as a series of major operations divided into three phases (prevention, response, and continual improvement), the theater antiterrorism campaign will move subordinate commanders beyond their defense-centric strategy. Establishing adequate physical security standards, transitioning through each campaign phase, prioritizing command installations and integrating existing plans are key elements of the campaign plan. Only when combatant commanders have well-developed--and exercised--response plans will U.S. Forces truly be prepared for the next terrorist attack.

BACKGROUND

> *"We must fight the attitude: 'It couldn't happen here'…*
> -- GEN (Ret) Henry H. Shelton, Former CJCS

Ever since the attacks on September 11, 2001, government leaders have continuously warned of future terrorist attacks. In May 2002, Governor Ridge, the Director of Homeland Security warned, "I don't think it's a question of if, it's a question of when," moments after delivering the commencement address at Carnegie Mellon University. "We'll do our best to make us safer and more secure, but we will not design a fail-safe system. It cannot be done."[1] One week later, the Associated Press reported General Ryan, CJCS, declared, "Just like a wounded animal is the most dangerous, they (al-Qaida) still pose a threat to our armed forces."[2] Six months later during Congressional testimony regarding Iraq and weapons of mass destruction (WMD), Secretary Rumsfeld warned, "Terrorist states have enormous appetite for these powerful weapons—and active programs to develop them. They are finding ways to gain access to these capabilities. This is not a possibility—it is a certainty. In word and deed, they have demonstrated a willingness to use those capabilities."[3]

So, if senior administration and military leaders are predicting future terrorist attacks with such a degree of certainty, why aren't forces more prepared? Why do commanders' efforts continue to focus on preventing or deterring a terrorist attack with little or no regard to recovering from the inevitable attack and its impact on mission capability?

Effectively protecting the forces requires maintaining mission capability and an ability to respond to, and recover from, a terrorist attack, regardless of whether the attack is at home-station, in-transit or at a deployed site. Military forces may have plans to prevent an attack, but not getting ready for prevention to fail is dangerous. The adage "Failing to plan is

planning to fail," is more than just rhetoric. Preparing to recover from terrorist attacks is becoming ever more critical as U.S. Forces expand their global footprint.

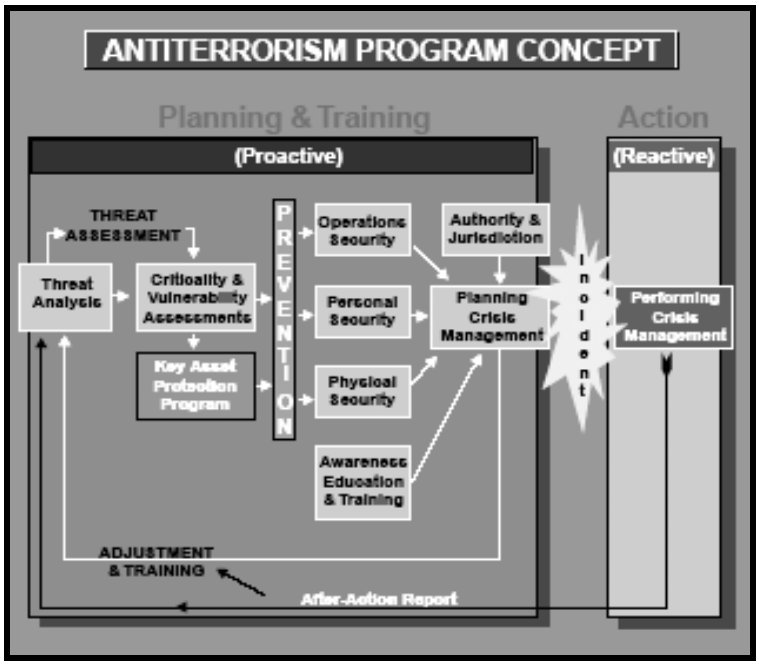
The intent of this paper is to define the problem with identifiable references; examine national strategies with regard to terrorism; analyze lessons learned from past terrorist attacks; and finally, fuse the outcome into a theater strategy for an effective antiterrorism[4] (AT) program. This paper will demonstrate how applying operational art can shift the solely defensive mindset of commanders to better protect U.S. Forces.

DEFINING THE PROBLEM

In order to understand the inherent problems with a defensive mindset, one must know the elements of an AT program and recognize the enemy threatening the military force.

Understanding the Program Elements

Joint Publication 3-07.2 identifies proactive and reactive elements in an antiterrorism program. As shown below, the proactive element includes those essential programs to prevent an attack, but the reactive component will save lives following an attack. [5]



Joint Publication 3-07.2, page IV-2

While subordinate commanders may have some partial response capability, theirs will be quickly overwhelmed by any type of terrorist attack with the possible exceptions of a small bombing, an assassination, or some other limited terrorist event. In most cases, the subordinate commanders rely on the combatant commander who has the assets and capacities to coordinate a major response effort. Therefore, the critical element of a theater antiterrorism program is the response capability--not the ability to defend against an attack.

Understanding the Threat

In order to break the defensive paradigm, planners must recognize the threat capabilities presented by terrorists are really not new. Some might argue suicide pilots flying into buildings are a new threat, but one only has to recall the kamikaze pilots of WWII to counter the argument. Consider for example, one threat to U.S. installations during the Cold War - a Spetsnaz team. The Spetsnaz, a Russian Special Forces unit, consisted of small, well-armed teams trained to destroy their enemies' key facilities or mission capabilities, i.e. weapons delivery, fuel storage, or communication systems. For years, training doctrine has included defending against small team tactics or an opposing force possessing chemical and biological weapons. During the Cold War, commanders planned for small unit attacks and recognized the probability of the defenses failing. In fact, many U.S. exercises included scenarios to defend against, respond to, and *recover* from a Spetsnaz attack. Why then, are non-state actors with similar capabilities and tactics perceived as a unique adversary requiring exclusive physical security systems costing billions of dollars? Is today's terrorist threat to an operational commander's mission so much different than the threat a Spetsnaz team presented? In actual fact, terrorists do not present a new threat but simply another, albeit less predictable, threat to different targets.

The greatest distinction between conventional enemies and today's terrorist is primarily the target of their attacks. Conventional enemy forces, like those encountered during the Cold War, targeted legitimate military objectives, whereas today's terrorist does not appear to have similar restraints. Another distinctive characteristic is the unpredictable nature of terrorists which understandably reinforces a commander's desire to prevent an attack. Ironically, the lack of indications and warning of an attack which drives many to a greater reliance on strong defenses is precisely the reason why preparing a response plan is crucial.

The criticality of response plans is evident in national strategies which reveal a persistent theme of preparedness to complement senior officials' warnings of expected terrorist attacks.

NATIONAL SECURITY STRATEGIES

> *"The terrorists continue to plot against us. They still want to harm us."*
> -- President Bush remarks on the War on Terror
> Port of Charleston, South Carolina, 5 Feb 2004

Current national strategies with respect to terrorism include the National Security Strategy, National Strategy for Combating Terrorism and the National Strategy for Homeland Security. A review of each strategy explicitly illustrates one overarching principle of our combating terrorism policies--an imperative to prepare a terrorist attack response capability.

The National Security Strategy (NSS) divides terrorism into two distinct types, conventional and weapons of mass destruction (WMD). With respect to conventional terrorism, the approach is an offensive, or counterterrorist, strategy. Specifically, the NSS states, "Our priority will be first to disrupt and destroy terrorist organizations of global reach and attack their leadership; command, control, and communications; material support; and finances. This will have a disabling effect upon the terrorists' ability to plan and operate."[6]

The underlying strategy is to defeat conventional terrorism using each of the national instruments of power (diplomatic, informational, military and economic).

However, the most dangerous terrorist attack would be one involving WMD and the NSS clearly identifies a comprehensive strategy including:

- Proactive counter-proliferation efforts
- Strengthened nonproliferation efforts to prevent rogue states and terrorists from acquiring the materials, technologies, and expertise necessary for weapons of mass destruction
- Effective consequence management to respond to the effects of WMD use, whether by terrorists or hostile states [7]

The consequence management strategy clearly advises, "the United States must also be prepared to respond to the effects of WMD use against our forces abroad, and to help friends and allies if they are attacked."[8] The national strategy obliges one to accept the reality of a WMD event and requires preparation to recover from such an attack.

Like the NSS, the National Strategy for Homeland Security (NS-HLS) also advocates readiness. With respect to readiness, the NS-HLS states, "We must prepare to minimize the damage and recover from any future terrorist attacks that may occur despite our best efforts at prevention. Past experience has shown that preparedness efforts are key to providing an effective response to major terrorist incidents and natural disasters." [9]

The National Strategy for Combating Terrorism (NSCbT) also addresses the significance of preparing a response capability. The NSCbT identifies the strategic intent is to stop terrorist attacks against the United States and its allies based on four fronts: *defeating* the terrorist organizations through offensive actions, *denying* sponsorship and safe havens, *diminishing* conditions fostering terrorism and, *defending* the United States and its citizens. The latter is characterized as the most important and includes, "extending our defenses to

ensure we identify and neutralize the threat as early as possible."[10] Identifying defense as the most important front to combating terrorism seems to agree with the defensive mindset of combatant command and component staffs. But, the NSCbT also identifies preparedness as a specific objective of the goal to protect U.S. citizens at home and abroad. Specifically, the NSCbT states, "…solid plans, preparations, and immediate response remain key to mitigating acts of terrorism. Unity of effort requires coordination not only at the apex of the federal government, but also at the operational/tactical level…"[11] So, if the national strategies which drive military strategy advocate preparedness in addition to defense, why does the military culture place so much emphasis on the defense? The answer may be found in the tangible benefit of defenses whereas preparedness is more difficult to gauge. The idea of creating impermeable defenses is embedded in military culture. However, that idea, when coupled with the confidence derived from military superiority, creates a dangerous set of conditions. Unfortunately, those conditions may have contributed indirectly to previous terrorist attacks.

LESSONS LEARNED FROM TERRORIST ATTACKS

> *"Unless we learn, disseminate, and apply the lessons learned about terrorism, we will repeat the tragedies of the past."*
> -- GEN (Ret) Wayne A. Downing

The United States has endured several terrorist attacks during the last twenty years and, regrettably, history suggests the military is slow to put into practice the lessons learned from those events. Preventing attacks is critical, but while U.S. forces continually improve security, one enduring fact remains - regardless how well they are built, defenses are not impenetrable. Despite our best efforts, terrorists defeated existing military defenses to kill Marines in Lebanon (1983), soldiers in Saudi Arabia (1995), airmen in Saudi Arabia (1996)

and sailors in the Gulf of Aden (2000). Three of the attacks resulted in major investigations and the lessons learned remain problematic today.

October 23, 1983 – Bombing Of Marine Barracks

The need for prepared responses at the operational level was blatantly obvious in 1983 following the bombing of the Marine Barracks in Beirut. The investigation revealed a lone terrorist drove an explosive-laden vehicle through the open, manned compound gate into the barracks lobby before detonating the explosives. The Long Report determined Combined Task Force 61 (CTF 61) initiated their mass casualty plan immediately following the bombing and credited them with saving many lives due to their "well-understood and frequently exercised" plan.[12]

However, the report identified several problems with the higher headquarters (U.S. European Command) execution of their medical evacuation plans. Existing procedures at the time directed medical patients to U.S. military hospitals in Italy or Germany--over 4 hours away--despite CTF 61 intention to evacuate the most serious patients to the prepared and ready British Royal Air Force (RAF) hospital at RAF Akrotiri, Cyprus--a 1-hour flight. Patient evacuations were further compounded by a delay in obtaining medical supplies for the C-9 aircraft at Incirlik Air Base, Turkey. The aircraft eventually arrived in Beirut two hours later than the estimated time of arrival. Finally, the med-evac flights to Germany were directed to Rhein-Main Air Base rather than Ramstein Air Base, the closest base to the Landstuhl Medical Facility. The Rhein-Main decision required additional travel time for the most seriously wounded. The report concluded, "knowledge of regional medical facilities and potential sources of support was poor, and overall medical planning was inadequate."[13] Preparedness was an issue in 1983 and 13 years later, the Downing Assessment Task Force

identified similar issues following the attack against the U.S military compound in Dhahran, Saudi Arabia.

June 25, 1996 – Bombing Of Khobar Towers

The Downing Report of the Khobar Towers bombing found the emphasis of force protection efforts was on preventing penetration of the perimeter by a car, truck, man-pack suicide bomb, or a letter or package bomb.[14] Learning from the Marine experience in Beirut, U.S. Forces built robust access control points and effectively prevented unauthorized access onto the military compound. The terrorists adapted to the U.S. Forces' defensive measures by detonating a large vehicle-borne improvised explosive device (VBIED) at the perimeter near the military apartments.

The lessons learned report identified a need for preparedness, in addition to several procedural issues such as poor cooperation with Host Nation, ineffective intelligence, and a lack of training exercises to respond to terrorist attacks. Specifically, the Downing Report stated "mass casualty procedures could be improved" and recommended commanders "continue emphasis on realistic mass casualty training and exercise scenarios."[15]

October 12, 2000 – Bombing Of the USS Cole

Four years later the Cole was attacked in the Gulf of Aden in a similar tactic as was used in Beirut and Khobar, the terrorists detonated an explosive-laden vehicle (a boat) alongside the U.S. warship. Even though the incident occurred four years after the Khobar attack and nearly *17 years* after the Beirut bombing, the Cole Commission report again found the combatant commander, this time U.S. Central Command, was not prepared to respond to such an event. The report suggested geographic combatant commanders "get out of the purely defensive mode" and "identify theater rapid incident response team requirements and

integrate their utilization in contingency planning for in-transit units." [16] The report also recommended, "Incident response must be an integral element of AT/FP planning."

In each of these three events, a similar method of attack defeated military defenses and each time the combatant command staff was ill-prepared to provide a response capability.

ASSESSMENT OF CURRENT ANTITERRORISM PROGRAMS

> *"From the National Command Authorities to the team leaders in the field, force protection is a primary function of command. That responsibility demands that we take the protection of our forces against terrorism into consideration when we are developing our policies, structures, budgets, facilities and every operations plan."*
>
> -- GEN (Ret) Wayne A. Downing

A commanders' obligation to develop--and exercise--incident response plans is glaringly obvious from lessons learned. Notwithstanding the reports, combatant commanders continue to advocate on behalf of their Service components for millions of dollars to defend against attack without a comparable effort to develop plans to respond to an attack.

In November 2002, the Government Accounting Office (GAO) estimated Service funding for combating terrorism between FY99 and FY03 amounted to over *$8.4 Billion dollars*![*] The GAO report acknowledged, "it is widely recognized that vulnerabilities at military installations will continue to outpace available funding."[17] The continuously rising costs are reflected in U.S. Pacific Command's (USPACOM) annual AT/FP unfunded requirements list. The USPACOM Commander identified 1044 security projects for his subordinate commanders totaling nearly $1.5 billion dollars for FY 04-09.[18]

[*] The report estimated $8.4B (excluding personnel costs) of the $32B DOD combating terrorism funding for FY99-03 was for other appropriations, i.e. procurement, research and development, and military construction.

While the subordinate commanders were pursuing greater defensive capabilities, the Joint Staff reported the following trends subsequent to Joint Staff Integrated Vulnerability Assessments (JSIVAs) in 2002:[†]

- Antiterrorism plans did not address the full spectrum of terrorist threats, did not include procedures for coordinating with outside responding forces, and did not include procedures to determine the nature and scope of incident response
- Threat assessments had not been conducted or did not identify terrorist capabilities and tactics, WMD assessments not conducted or did not identify all potential threats
- Exercise plans did not exist or were not fully developed, exercises did not include incident response or consequence management[19]

The Defense Threat Reduction Agency (DTRA) is one tool to assess the effectiveness of the combatant commanders' antiterrorism programs. The trends indicate subordinate commanders' do not always know what threats to defend against, remain transfixed on prevention through defense, and do not develop response plans. Demonstrating an executable response to mitigate the effects of known terrorist capabilities can prove to be an excellent deterrent to an attack. So, how does the combatant commander break the "bunker mentality" and move beyond a defense-based antiterrorism program?

RECOMMENDATIONS[‡]

Translating national strategies against terrorism into theater strategy is one responsibility of the combatant commander and his staff. Research suggests subordinate commanders continue to struggle with the concept of developing an executable antiterrorism program with

---

[†] Joint Staff provides annual report as a tool to improve AT programs. The Joint Staff classifies DTRA findings as trends if they are discovered at 20% of installations assessed during the calendar year. The actual number of findings and percentages are CONFIDENTIAL.

[‡] The recommendations in this paper are not intended to be portrayed as either the absolute solution or the all-inclusive answers to address the growing, ever-present terrorist threats. Rather, these suggestions are simply offered to provide the operational commanders with alternate planning considerations in their antiterrorism programs.

a viable responsive capability. To be effective, a combatant command staff should integrate lessons learned from previous attacks and results of current program assessments into the theater antiterrorism program. The most significant of the following recommendations requires combatant command staffs to view a viable antiterrorism plan as not another administrative program, but rather a series of military operations requiring the essence of operational art.

Notional Antiterrorism Campaign Plan

The campaign planning construct is ideal for providing the combatant commanders' vision for his antiterrorism program. Joint Publications 3-0, Doctrine for Joint Operations states:

> "A campaign is a series of related major operations that arrange tactical, operational and strategic actions to accomplish strategic and operational objectives. A campaign plan describes how these operations are connected in time, space, and purpose. Within a campaign, major operations consist of coordinated actions in a single phase of a campaign and usually decide the course of the campaign"[20]

Operational commanders should view antiterrorism, as a long-term, phased campaign requiring related major operations at each level of command from the operational combatant command staff down to the tactical installation and facility-level. The sequenced operations should lead to achieving theater and strategic objectives.

The first phase of the campaign could be prevention with an objective of providing adequate security at each installation and in-transit facility. Once achieved, forces transition to the second phase to develop response and recovery plans. Exercising well-developed, coordinated response plans to include Host Nation (Federal and state authorities in the U.S.) throughout the theater is the objective of the second phase. Finally, the third phase would

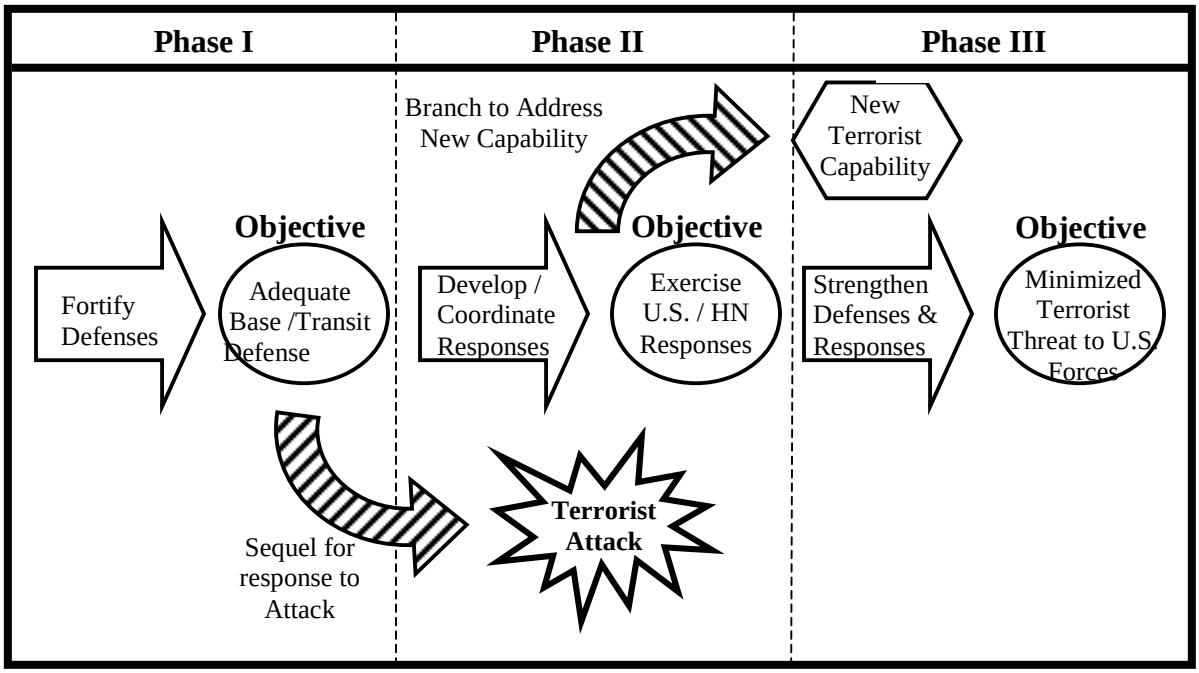
provide continuous improvement of processes to maintain a high state of readiness regardless of changes in terrorist tactics or procedures.

Plans should include sequels to react to an attack as well as branches for counterterrorism operations and to address new enemy capabilities, e.g. acquisition of biological agents. For instance, if the combatant commander's intelligence staff assessment initially determines the most likely terrorist threat is a VBIED and terrorists do not possess the ability to employ a biological weapon, the main effort should be toward protecting against and responding to the VBIED threat. Planners should nonetheless develop branches to counter the biological threat in case the assessment changes all the while moving forward in the campaign planning.

The key to a successful antiterrorism campaign is to view the effort in phases with an absolute imperative to move from one phase to the next. By sequencing events, the combatant commander will ensure subordinate commanders reach the desired objective within established timelines. In order to influence some of the considerations in the factor of space (political sensitivities, geography, sovereignty issues), the combatant command must coordinate the efforts with HN and other U.S. agencies in his area of responsibility (AOR).

Since combatant commands already have mature antiterrorism programs, each might be in a different phase of the campaign plan today, but each phase remains essential. Regardless of the phase commanders are in today, the expanding global footprint and increasing number of new "bases" will require some to initiate new programs through the first phase of the campaign. This notional antiterrorism campaign plan should remain a relevant and continuous operation throughout the Global War on Terrorism.

A graphic illustration of a notional antiterrorism campaign plan with an example of significant actions follows:



Phase I Prevention	Phase II Recover and Respond	Phase III Continual Improvement
- Assess threat - Identify critical assets and impact on mission - Determine acceptable levels of risk - Identify minimum standards & program actions: -- Organize, train, equip security forces -- Address critical APOD / SPOD[§] vulnerabilities -- Strengthen facilities to mitigate threats - Improve intelligence capabilities	- Train, equip incident response teams - Coordinate U.S. Forces theater response plans - Assess Host Nation (HN) / U.S. state capabilities - Coordinate combined U.S. / HN theater response plans - Exercise and evaluate combined response plans - Develop alternative areas and mission capabilities to counteract for losses from terrorist attack	- Train, equip HN or State emergency response teams - Assess effectiveness of plans - Review lessons learned and revise plans - Incorporate lessons from testing, exercising, experience with actual incidents, and technology advancements

[§] Air Ports of Debarkation/Sea Ports of Debarkation

Appropriate Level of Security: Absolute or Adequate?

DOD Directive 2000.12, DOD Antiterrorism Program, charges the geographic combatant commander with overall antiterrorism responsibility in his AOR, to include establishing prescriptive standards and assessing the effectiveness of subordinate programs.[21] Those standards should identify adequate physical security to address known threats. The operative word is adequate--physical security will never defeat all potential terrorist threats, so combatant commanders should develop effective physical security standards with an acceptable level of risk. A determined terrorist can slowly negotiate the serpentine barriers, shoot the armed guards at the gate and detonate a large VBIED at a mission-critical facility on nearly any military installation at 0400.

Determining an acceptable level or risk and preparing options to operate without a damaged mission-critical facility is a practical course of action. While the combatant commander does not provide funding, it is the combatant commander who advocates for subordinate commanders when the Services do not adequately fund critical issues. Commanders cannot continue to spend billions of dollars in an imprudent attempt to protect against all possible threats. Admiral Fargo, the Commander, U.S. Pacific Command acknowledged, “If you try to cover the whole landscape, not only will you fail, you'll dilute your effectiveness. So you have to worry about what you need to worry about.”[22] What commanders should worry about is providing an adequate level of security supported with appropriate response plans to counter known terrorist threats. Since the combatant commander has a theater perspective, he is more able to synchronize efforts, allocate resources and facilitate procurement actions to protect forces and mission capability. Identifying clearly defined objectives and firm dates to transition to the next phase allows the

combatant commander to influence the factor of time as he pursues his antiterrorism campaign in addition to exercising his control of forces.

Transitioning Beyond Defense

In order to effectively protect forces, combatant commanders should establish not only minimum standards of protection but also closing dates to implement the standards. An unambiguous "no later than" date to establish adequate physical security will allow subordinate staff planners to visibly see the end of one phase in the campaign and a transition to the next. Once all subordinate commanders report meeting the objectives of the current phase, the combatant commander can initiate the next phase of the campaign. Similar to the Joint Staff's declaration of calendar year 2000 as the *Year of the Antiterrorism (AT) Plan,*[23] the combatant commanders' could designate an appropriate time for each phase to keep the command efforts focused on the objective. Each phase should consider the timelines of the Planning, Programming, and Budgeting System (PPBS). Naturally, commanders would not be prohibited from strengthening their defenses through small acquisition efforts or improving their tactics, techniques and procedures. The intent of the phasing is primarily to prevent static defensive plans or the stagnation of antiterrorism efforts. In addition, the changing, unpredictable nature of the terrorist threat and limited available resources will require commanders at all levels to prioritize their efforts.

Prioritize Installations and Ports

Each installation (bases, housing areas, support facilities) and ports of debarkation (air and sea) are critical facilities in the eyes of the individual commanders, so combatant commanders should consider prioritizing each location to balance resource allocation during the campaign. Understandably, individual commanders desire the best level of protection for

personnel and resources under their command. Some commanders who are well-versed in the resources process may be better able to provide a greater level of security when in fact another installation or port is more critical to the operational commander. The necessity for prioritizing military installations became apparent following the 9/11 attacks and the reported anthrax incidents. So many commands throughout DOD attempted to procure protective masks and ensembles, the requirements overwhelmed the market capacity[24]. The staff with the theater perspective knows best where to focus critical capabilities and is in the best position to identify and mediate competing requirements between Service components or DOD Agencies.

Identify and Integrate Existing Plans

Identifying capabilities of organizations, to include non-governmental organizations (NGOs), private volunteer organizations (PVOs) and other government agencies (OGAs), and integrating their existing plans into the theater antiterrorism campaign is critical. The National Strategy to Combat Weapons of Mass Destruction (National Security Presidential Directive 17) established an office to coordinate and improve "U. S. efforts to respond to and manage the recovery from terrorist attacks outside the United States" and it is the combatant commander who is in the best position to fit military capabilities into the interagency process.[25] The synergistic effect of combining U.S. military and HN (or Federal, state agencies in the U.S.) antiterrorism efforts will provide the additional benefit of improving response capabilities to other emergency situations (e.g. natural disasters, humanitarian aid or disaster relief).

Determining responsibilities of all elements down to the tactical (installation) unit or non-military organizations, synchronizing movements and exercising plans are vitally important

before an event requires action. The mere existence of a resource like a Fleet Antiterrorism Security Team does not ensure the capability will be available when needed. Unless individual units, including NGOs, PVOs, and OGAs, are aware of their integrated role and exercise together, the plan may not work as effectively as possible. For example, the Naval Hospital at NAS Rota, Spain maintains a deployable surgical team on stand-by for 30 days with the planned capability to respond anywhere in the EUCOM AOR within 24 hours. However, a current Naval War College (NWC) student and former member of the NAS Rota team reported the medical team lacks organic airlift, logistic support, and force protection capabilities. If called upon for an actual emergency, the former member doubted the team could meet planned expectations.[26] In fact, a similar team was deployed to the 1998 earthquake in Turkey. According to another NWC student who was responsible for deploying the 1998 team from NSA Naples, Italy, the team arrived late and without force protection assets due to the absence of the necessary combatant command support.[27] Admittedly, the team was not deploying to a terrorist attack in 1998, but the result of a large VBIED like the one used at the Khobar Towers does not differ much from the aftermath of an earthquake - buildings collapse and people are injured or killed. While this is only one example of the lack of integrated planning, it suggests the combatant command staff forgot the lessons learned 15 years earlier following the Beirut bombing. Synchronizing assets into coordinated emergency response plans is critical for peacetime disasters and will prove significant when needed to respond to a terrorist attack. To be effective, though, the plans must eventually be exercised as executed, not simply "chalk talks" or paper exercises.

CONCLUSION

> *"…there are real dangers in confronting a tyrant who has and uses weapons of mass terror and has links to terrorists. But those dangers will only grow. They are far greater now than they would have been five or ten years ago, and they will be much greater still five or ten years from now."*
>
> -- DepSecDef Wolfowitz, 23 Jan 03

The threats continue to grow, so combatant commanders must develop more effective antiterrorism programs. To be effective, a combatant commander's antiterrorism program must provide not only a defensive capacity, but more importantly, a coordinated response when prevention fails. Lessons learned from previous terrorist attacks against U.S. Forces have revealed the imprudence of attempting to protect through defenses alone since terrorists will adapt their methods to defeat security measures. Combatant commanders must break the enduring "prevention through defense" paradigm given that defending against all possible threats is not only costly, it is impossible! One way to shift the military mindset is to view the Global War on Terrorism as analogous to the Cold War creating a more familiar scenario for staff campaign planning.

By employing campaign planning principles, the combatant commander can make clear his strategic vision for a proactive and reactive antiterrorism program. The phased campaign plan should include specific major operations in each phase, clearly articulated objectives and timelines. If successful, it will focus and sequence subordinate unit actions (ways), identify what assets are or will be available (means) and finally, demonstrate how the commander intends to achieve his ultimate objective of protecting the force and his mission capabilities (ends). By applying operational art through an effective antiterrorism campaign plan, the combatant commander can ensure his forces are prepared when the next terrorist attack occurs.

NOTES

[1] James O'Toole, "'Not if, but when:' Ridge warns that another terror attack is inevitable," Pittsburgh Post-Gazette, 20 May 2002, < http://www.post-gazette.com/nation/20020520ridge0520p1.asp>, [4 Jan 04].
[2] Matt Kelly, "Rumsfeld: Terrorists Inevitably Will Get Nukes," St Augustine Record, 22 May 2002**,** < http://www.staugustine.com/stories/052202/nat_731775.shtml >, [4 Jan 04].
[3] Donald H. Rumsfeld, "Prepared Testimony," U.S. Congress, House, House Armed Services Committee, U.S. Policy Towards Iraq, Hearings before the House Armed Services Committee, 107th Cong, 2d sess., 18 September 2002. < http://www.defenselink.mil/speeches/2002/s20020918-secdef.html>, [4 Jan 04].
[4] Combating Terrorism (CbT) is defined in Joint Publication 0-1 as: Actions, including *antiterrorism*…and *counterterrorism*…, taken to oppose terrorism throughout the entire threat spectrum. JP 0-1 defines Antiterrorism (AT) as *defensive* measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces and counterterrorism (CT) as *offensive* measures taken to prevent, deter, and respond to terrorism.
[5] Joint Chiefs of Staff, Joint Tactics, Techniques and Procedures for Antiterrorism, Joint Publication 3-07.2, (Washington, DC: 17 March 1998), IV-2.
[6] President, The National Security Strategy of the United States of America**,** (The White House: 2002), 5.
[7] Ibid., 14.
[8] Ibid.
[9] President, The National Strategy for Homeland Security, (The White House: 2003), x.
[10] President, The National Strategy for Combating Terrorism**,** (The White House: 2003), 11-12.
[11] Ibid., 27.
[12] Department of Defense, DOD Commission on the Beirut International Airport (BIA) Terrorist Act of 23 October 1983 (Washington, DC: 1984), 110-13.
[13] Ibid.
[14] Department of Defense, Report of the Assessment of the Khobar Towers Bombing (Washington, DC: 1996), 56.
[15] Ibid., 42.
[16] "DoD USS COLE (DDG 67) Commission Report," 21 January 01, Department of Defense Publications, <http://www.defenselink.mil/pubs/cole20010109.html>, [3 Jan 04].
[17] General Accounting Office, Combating Terrorism: Actions Needed to Guide Services' Antiterrorism Efforts at Installations, Report to the Chairman, Special Oversight Panel on Terrorism, Committee on Armed Services, House of Representatives (Washington, DC: 2002), 15.

[18] CDR Tom Graziano, "PACOM J30 AT/CIP Briefing," 21 June 2002, Joint Staff Deputy Directorate for Global Operations Antiterrorism and Force Protection FY 04-09 Resource Requirements Briefing, <http://www.nmcc.smil.mil/j34/terrorism/Library/Accessible/DocsPubsPresentations/ConferencesSeminars/RR_Meeting/CINCs/PACOM.html>, [8 Jan 04].
NOTE: This is UNCLASSIFIED data from the SIPRNET.
[19] Joint Chiefs of Staff, Deputy Directorate for Global Operations Antiterrorism and Force Protection Message, Joint Staff Integrated Vulnerability Assessment (JSIVA) Trends for the Twelve Month Period of Calendar Year (CY) 02, 31 January 2003, <http://www.nmcc.smil.mil/j34/terrorism/Library/Assessments/Trends/CY02_JSIVA_Trends.txt>, [8 Jan 04].
NOTE: This is UNCLASSIFIED datafrom the SIPRNET.
[20] Joint Chiefs of Staff, Doctrine for Joint Operations, Joint Publication 3-0, (Washington, DC: 10 September 2001), III-4.
[21] Department of Defense, DoD Antiterrorism (AT) Program, DODD 2000.12, August 18, 2003.
[22] Thomas B. Fargo, (speech presented at the Homeland Security Conference, Honolulu, Hawaii, 21 November 2003), USPACOM Speeches and Transcripts < http://www.pacom.mil/speeches/sst2003/031121hsc.shtml>, [12 Jan 04].
[23] General Shelton, former Chairman, Joint Chiefs of Staff, designated the *Year of the AT Plan* after discovering several installations failed to develop plans as directed within the 3-year time limit subsequent to the Downing Report. In a "Personal For" message to the combatant commanders, the Secretary of Defense directed them to report the status of all their installation AT plans. The reports were a prerequisite to the CJCS testimony to a Congressional committee.
[24] Eventually, the Joint Staff recognized the dilemma and attempted to cease all further acquisitions of any chemical/biological equipment until they could prioritize requirements throughout DOD. The prioritization effort took months to complete and all the while, installations continued to order equipment by avoiding the Joint Staff process. Today, the top 200 installations in DOD are prioritized for CBRNE purposes, but the prioritization methodology excluded APODs/SPODs.
[25] President**,** National Security Strategy to Combat Weapons of Mass Destruction**,** (The White House 2002), 5.
[26] Doctor (CDR) David Lane, Naval War College student, interview by author, 29 January 04, Naval War College, Hewitt Hall, Newport, Rhode Island.
[27] LCDR Debra Duncan, Naval War College student, interview by author, 29 January 04, Naval War College, Hewitt Hall, Newport, Rhode Island.

BIBLIOGRAPHY

Duncan, Debra, LCDR. Student, Naval War College. Interview by author, 29 January 04. Naval War College, Hewitt Hall, Newport, Rhode Island.

Gurr, Nadine and Cole, Benjamin. The New Face of Terrorism. Threats from Weapons of Mass Destruction. London: I.B. Tauris Publishers, 2001.

Hoge, James F., Jr., and Gideon Rose, eds. How Did This Happen? Terrorism and the New War. New York: Public Affairs, 2001.

Lane, David, Dr. (CDR). Student, Naval War College. Interview by author, 29 January 04. Naval War College, Hewitt Hall, Newport, Rhode Island.

Laqueur, Walter. The New Terrorism. Fanaticism and the Arms of Mass Destruction. New York: Oxford University Press, 1999.

Lesser, Ian O., United States. Air Force., Rand Corporation., and Project Air Force (U.S.). Countering the New Terrorism. Santa Monica, CA: Rand, 1999.

United States. President. National Security Strategy to Combat Weapons of Mass Destruction**.** Washington, DC, White House, 2002.

United States. President. The National Security Strategy of the United States of America. Washington, DC, White House, 2002.

United States. President. The National Strategy for Combating Terrorism**.** Washington, DC, Executive Office of the President, 2003.

United States. President. The National Strategy for Homeland Security. Washington, DC, White House, 2003.

U.S. Congress. House. House Armed Services Committee, U.S. Policy Towards Iraq: Hearings before the House Armed Services Committee. 107th Cong, 2d sess., 18 September 2002.

U.S. Department of Defense. DoD Antiterrorism (AT) Program. DODD 2000.12. Washington, DC, 2003.

U.S. Department of Defense. DoD Antiterrorism Standards. DODI 2000.16. Washington, DC: 2001.

U.S. Department of Defense. DoD Commission on the Beirut International Airport (BIA) Terrorist Act of 23 October 1983. Washington, DC: 1984.

U.S. Department of Defense. DoD USS COLE (DDG 67) Commission Report. Washington, DC: 2001.

U.S. Department of Defense. Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence. DoD O-2000.12-H. Washington, DC: 1993.

U.S. Department of Defense. Report of the Assessment of the Khobar Towers Bombing. Washington, DC: 1996.

U.S. General Accounting Office. Combating Terrorism: Actions Needed to Guide Services' Antiterrorism Efforts at Installations. Report to the Chairman, Special Oversight Panel on Terrorism, Committee on Armed Services, House of Representatives. Washington, DC: 2002.

U.S. Joint Chiefs of Staff. Doctrine for Joint Operations. Joint Pub 3-0. Washington, DC: 10 September 2001.

U.S. Joint Chiefs of Staff. Joint Tactics, Techniques and Procedures for Antiterrorism. Joint Pub 3-07.2. Washington, DC: 17 March 1998.