1-1-2012

Continuity of Operations: A Strategy to Secure the Nation

Matthew J. Cassidy
Pace University

CONTINUITY OF OPERATIONS:

A STRATEGY TO SECURE THE NATION

BY

MATTHEW J. CASSIDY

SUBMITTED IN PARTIAL FULFILLMENT OF

REQUIREMENTS FOR THE DEGREE OF MASTER OF

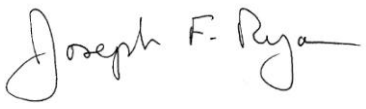
ARTS IN MANAGEMENT FOR PUBLIC SAFETY

AND HOMELAND SECURITY

DYSON COLLEGE OF ARTS AND SCIENCES

PACEUNIVERSITY

MAY 2012

APPROVED BY: 

Abstract

The sharing of power and responsibilities between the individual states and the federal government is detailed in the US Constitution and is called federalism. Research has indicated that the shift of power between the states and federal government has waxed and waned over the last 236 years. This qualitative study is based upon literature review of the relationships of local, state, and federal governments in responding to catastrophes. Each level of government brings unique capabilities to the response to catastrophic events. There is no need to usurp federalism in order to survive the next catastrophe; it is going to take all levels of government working together in a collaborative fashion. The aim of this study is to influence policy makers to take a more balanced approach to the roles of local, state, and federal governments in emergency management.

In the past two decades, the United States and its citizens have experienced several natural and man-made (terrorist) disasters. Devastating in their own right, each disaster has led members of society to question the capability of local, state, and federal officials. The economic climate in the United States has placed emergency management efforts and the progress made over the past few years in jeopardy. Significant budget cuts and limited funding provide many challenges to continue the progress in making communities safe, less vulnerable, and resilient in regards to disasters and catastrophic emergencies. This thesis proposes the use of increased collaborative arrangements, greater accountability, and the use of performance measures as ways to achieve greater efficiency to maximize emergency management efforts under budget constraints.

A better understanding of emergency plans and the effect it has had on varying levels of society will enable civic leaders an opportunity to improve existing emergency plans and reduce the potential for loss of life. Preparing civilians has more impact on the psychological well-being of the nation than being rescued by emergency services; and preparing civilian's increases community resiliency at a faster rate than preparing response personnel.

Acknowledgements

I wish to express my thanks to all my professors and classmates for their encouragement and guidance through the program. The feedback provided by my classmates has proven invaluable and help me to grow as I worked toward completing my degree. In particular, I wish to thank Dr. Joseph Ryan for his guidance and direction throughout my tenure as a graduate student at Pace; Professors Comisky and Littlejohn were exceptionally helpful with their feedback, comments and constructive criticism throughout my coursework. This feedback enabled me to move forward with confidence and complete my degree. Having professors that understand the unique challenges that student's face when they are also working full time and have other life commitments is essential. A successful graduate student needs support and guidance, and this is just what PACE provides to its students. My professors made me feel as if I mattered and worked with me to accomplish my goals.

I would also like to acknowledge my supervisor who gave me the final encouraging push to pursue this Master's degree program and the daily reminder that "if it were easy, everyone would have a Masters Degree". Finally, I would like to thank my family and friends who sacrificed a lot of time without me, so that I could work on my course work and projects. Your encouragement, support, and direction has helped me to achieve heights I could not have seen without your knowledge, patience, or caring guidance. In the end, you helped me to realize a simple truth: what you get out of something is directly related to what you put into it. I am better off for your efforts and I thank you. My parents, whom have always believed in me and have encouraged me to strive for excellence in every encounter and opportunity, I have inherited from them a strong work ethic, an appreciation and respect for truth, and a sense of decency.

Table of Contents

Chapter 1

Strategy: Continuity of Operations

"But I just think we've got such continuity with what we're doing that most people come in and fill in the blanks. And sometimes we leave a lot of blanks to be filled."

Charlie Hunter

Purpose

This Strategy Memorandum proposal provides a general overview of the Department of Homeland Security (DHS) Continuity of Operations. It provides an examination of planning, ensuring mission stability and continuation of essential functions and services across a wide range of potential events. These are required for emergency preparedness and response policies in regards to needs and populations, by allowing reduced interruptions of key enterprise services or command and control capabilities. This memorandum proposal details essential capabilities required to support functional areas, addresses circumstances that may cause a loss of essential capabilities, and assists leaders and staffs to plan for contingencies to maintain recovery mission essential functions and capabilities. An alternative for disconnected or interrupted services begins with an effective Continuity of Operations (COOP) plan to include provisions for Disaster Recovery.

This memorandum proposes a two-phased process for developing a Continuity of Operations plan. The process includes a near term and a longer term step:

Near term: review the planning to establish the foundation for a Continuity of Operations planning format and provide clear short term guidance to staff by clarifying government priorities.

Long term: design a process to test assumptions, create a comprehensive community vision and translate the Council's Continuity of Operations goals into an implementation plan to guide the course for the future.

The Department of Homeland Security, according to its assigned response mission, is to lead, manage and coordinate the national response to acts of terrorism, natural disasters, or other emergencies (DHS). The challenge for national preparedness is that the current system for homeland security does not provide the framework to manage the challenges posed by 21st century catastrophic threats. Under the current framework, the federal government merely coordinates resources to meet the needs of local and state governments based on their requests for assistance. The challenge for public safety and security is that the federal government provides assistance only when local agencies are overwhelmed or are depleted. The fundamental responsibility of public safety falls with local and state governments.

In February 2008 the former Secretary of Homeland Security Michael Chertoff signed the Federal Continuity Directive 2 (FCD 2) Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification and Submission Process. The last sentence of his directive states: "the provisions are applicable to all levels of federal executive branch organizations regardless of their location, and are also useful for state, local, territorial, and tribal governments and the private sector" (Chertoff).

COOP

An effective Continuity of Operations planning process has the potential to strengthen the shared understanding and commitment of any sized government, elected officials, and employees, and the community at large to the vision and goals for the community. The Federal Emergency Management Agency (FEMA) has provided a template and process for preparing for

Continuity of Operations; however, there is no clear guidance and direction to implement these plans (FEMA 1).

Modern COOP legislation is rooted in the November 1988, Executive Order 12656, Nov 88: "Our national security is dependent upon our ability to assure continuity of government at every level, in any national security emergency situation that might confront the Nation. . ." to include the survival of key leaders and order of succession; Continuity of Operations and of Mission Essential Functions; Relocation site(s); Protection of vital records/operating files; and the Ability to recover & reconstitute (executive Order). In addition, Presidential Decision Directive (PDD) 67, Oct. 98, further delineates COOP: the policy of the United States to have in place a comprehensive and effective program to ensure continuity of essential federal functions under all circumstances…" (PDD-NSC-67).

The terrorist events of September 11, 2001 have impacted the Homeland Defense and Security Policy. Domestic and national security emergencies include: fires, earthquakes, winter storms and ice, flooding, hurricanes, epidemics, highly contagious animal disease, drought, energy and fuel loss, hazardous material release, radiological accident, dam failures, explosion, volcanic eruption, sabotage, nuclear, chemical and biological terrorism, and weapons of mass destruction (1 DHS).

Continuity of Operations Program (COOP) is the ability of organizations to continue their mission essential functions with minimum operational interruption; this includes establishing responsibilities, policies, and planning guidance to ensure the effective execution of critical missions and continuation of mission essential functions (MEF) under all circumstances(1 DHS).

Mission Essential Functions (MEFs) are those functions of importance that must be performed during, and in the immediate aftermath of an emergency and cannot be postponed

longer than 24 hours. MEFs that cannot be executed may be transferred to another organization. There are a total of fifteen FEMA Emergency Support Functions (ESF) which provide the structure for coordinating federal interagency support for a federal response to an incident (1 DHS).

Although Continuity of Operations plans will vary in size and scope, they commonly include: a vision statement for the community and a corresponding set of goals and strategies for achieving that vision (1 DHS). The primary assumptions, based upon observed trends and conditions, may be highlighted to help explain and support the selected goals, and measurable indicators are central to determining if the desired vision is achieved (1 DHS).

The ability of local governments to continue their mission essential functions with minimum operational interruption include: planning, preparatory measures, responsive actions, and restoration to ensure the continuity of functions.

With the enhanced level of understanding provided by a Continuity of Operations plan, staff from all departments can be better equipped to achieve the government's prioritized near term and longer term goals. Because planning tends to relate work output to broader goals, employees have an opportunity to understand how their specific roles and levels of responsibility contribute to fulfilling the organization's vision. The plan can also become the basis for a performance management system throughout government organizations to strengthen responsibility (1 DHS).

Objectives of Strategy

It is impossible to properly plan for a disaster if the possibility impacts of various disruptions on an organization or agency are unknown. Assessing the impact of an event not only includes estimating the quantitative or economic losses but also the collective impact on the

organization's ability to operate, i.e. effects on personnel and the effect on the reputation of the organization.

Identify all functions: to begin the process of identifying functions within an organization, first identify the areas of responsibility. e the mission statement, values, goals and objectives, the organization chart, and a brief review of operating procedures, rulebooks and legal authorities (Federal Register).

A multi-year plan to enhance and refine the COOP plan and emergency readiness will need to be developed. This plan must include: short term and long term objectives, COOP needs, individual staff and unit roles, and timelines. The plan will be based upon objective information from testing, training exercises and implementation of COOP elements (FEMA1). Market the requirement to continue to employ COOP Planners by suggesting that a COOP Plan is an all hazards plan that must be a "living" document that is in a constant state of flux because of, among other things, changes in mission, personnel, IT capabilities, and regulatory requirements. An effective COOP Plan must be as current as possible, which means someone needs to keep up with those changes as they occur. To maintain viable COOP capabilities, state and local governments need to be continually engaged in a process to designate essential functions and resources, define short- and long-term COOP goals and objectives, anticipate and address issues and potential obstacles, and establish planning milestones, coupled with the exercise requirements state and local governments should be required to either create or assign a full time COOP planner/administrator.

Establish the Baseline

COOP plans can be activated in part or whole depending upon the disruption or threat. An event may demand that employees evacuate a single facility for a day or two, in which case

execution of the communications component of the COOP plan and IT recovery of data and systems only may be necessary. On the other hand, an organization's headquarters could be destroyed at the height of the business day, which will necessitate full execution of a COOP plan, including the deliberate and pre-planned movement of key personnel to an alternate work site that is capable of staining MEFs for a minimum of 30 days (MEF).

COOP plans outline an executive decision process for the quick and accurate assessment of the situation and determination of the best course of action for response and recovery in that case. Below is a sample of a decision matrix organizations can e in their COOP plan. For each area of responsibility identified, list the functions performed and provide a brief description of the activities typically completed in the identified function. COOP planners should collaborate with individuals from each division or branch of the organization and ask about the functions they and their coworkers perform on a daily basis.

Near Term Activity

Review the planning to establish the foundation for a Continuity of Operations Mission Essential Functions (MEFs). Senior management and the organization's COOP planner should determine the criteria for selecting MEFs. For example, if other organizations are dependent on a particular function to continue their operations, then the function is probably an essential function. Based on the pre-determined criteria, the COOP planner should go back to the previous list and for each of the functions listed under the various areas of responsibility indicate which ones are considered essential (MEF).

To determine Mission Essential Function Resource Requirements, examine the processes and services that support them. Each MEF has unique characteristics and resource requirements without which the function could not be stained. Those processes and services described for each

function that are necessary to assure continuance of an essential function are considered critical. Often critical processes and services vary depending upon the emergency or if they have a time or calendar component. For example, a wind storm would make debris removal a critical service, while a local power outage would possibly require generators, service crews, mutual Aid Agreements and Memoranda of Agreement/Understanding (MOA/MOU's). Likewise, debris removal may be a critical service in the spring or fall, but not in winter or summer (MEF).

Prioritize Essential Functions. Once all MEFs and their supporting critical processes and services have been identified, prioritize the functions according to those activities that are critical to resuming operations when a catastrophic event occurs. A MEF's time criticality is related to the amount of time that function can be suspended before it adversely affects the organization's core mission (MEF). Deciding which MEF should be restored first in a crisis would be impossible without also considering related critical processes and services, primarily those that mt be resumed soon after a disruption, generally within 24 hours. In addition, those functions upon which others depend should also receive a high priority in the sequence of recovery.

For each hazard, emergency managers should have a pre-established checklist that provides answers to the following questions, including such things as: vendor and partner agency agreements or relationships; software and supplies/equipment issues; workstation needs; vital records and documents required; and communications with organizations and critical customers.

Long Term Activity

Long term plan maintenance should be undertaken carefully, planned for in advance and completed according to an established schedule. Changes to organization structure, mission or essential functions should be made to the plan as they occur. Don't wait until you have an incident. Organizations should establish a review team designated to oversee plan review and

revision. Personnel selected for the review team need to have knowledge of overall organization operations; expertise in specific essential functions; expertise in specific advisory areas. The review team should meet on a regular basis throughout the year and after each exercise with each meeting structured to review all aspects of the COOP plan and should include action items for review and revision as necessary (FEMA 1).

Most major issues affecting COOP plans will result from lessons learned from exercises. Other sources of information may come from, depending on the level of government, Presidential Directives and/or state Emergency Management Offices or even corporate headquarters in the private sector, as appropriate, such as direction from organization leadership; policy or mission changes; changes in technology or office systems.

COOP plans and procedures should be coordinated, updated, validated and re-issued at least every 2 years, and a copy submitted to the organization's next level in their hierarchy. Additional reviews should be undertaken following each exercise and the testing of major systems. Issues raised in training may also trigger plan review (1 DHS).

Training

For the organization COOP program to be effective each element must know how to execute its portion of the COOP plan and how it relates to the other elements of the organization. Training and testing phases of the planning process are extremely important in regards to personnel awareness and readiness. They ensure that the organization's COOP program and all personnel are capable of supporting the continued execution of its MEFs throughout the duration of emergency situations. The objectives of the COOP training and testing program should include: assessing and validating COOP plans, policies and procedures; ensuring that personnel are familiar with COOP procedures; ensuring that COOP personnel are sufficiently trained to

carry out MEFs in a COOP situation; and testing and validating equipment to ensure both internal and external interoperability.

Before the COOP plan is exercised, personnel must be trained so that they know what their responsibilities are and have the skills and knowledge necessary to carry out their tasks. Training encompasses a range of activities, each intended to provide information and refine skills. Orientations are usually the first type of training conducted. They are typically presented as briefings. Orientations are a good way of introducing the general concepts of the COOP plan as well as announcing staff assignments, roles and responsibilities and describing how the COOP plan will be tested and exercised.

COOP training will be conducted annually. Training will consist of two sections: first, all staff with COOP specific roles will be trained in the roles and responsibilities contained in the plan; second, staff members who may be asked to assume roles not typically performed will receive an orientation on their other duties.

The Emergency Management Institute (EMI), located at the National Emergency Training Center in Emmitsburg, MD offers a broad range of on-line NIMS-related trainings. COOP Action Officers would need to complete the FEMA IS 546 COOP Awareness course that takes approximately 1 hour to complete, and the 4-hour FEMA IS 547 Introduction to COOP course. There is no cost for these courses, just time and the desire to learn and be prepared. The web site that can be provided to an organization's employees' is http://training.fema.gov/. Once at the site the new enrollees need only follow the instructions. Some of the courses do have prerequisites, normally they are the IS 100, 200, 700, and 800. All of those courses are on-line at no cost to the organization.

After familiarizing personnel with basic policies and procedures, hands-on training can provide practice in specialized skills, allow for practice of newly acquired skills, and help maintain proficiency for infrequently used skills (MEF).

Testing and Exercises

Tests are conducted to evaluate capabilities, not personnel. By testing, organizations can tell if the policies and procedures work as they should, when they should. Testing results should be published, and any identified gaps should be actively tracked and managed. Testing is critical for: alerts, notification and activation procedures; communications systems; vital records and databases; information technology systems; and reconstitution procedures (COOP Training).

The primary purpose of an exercise is to identify areas that require additional training, planning or other resources. Exercise results should be published and any gaps should be actively tracked and managed. The goals of a COOP exercise are to discover planning weaknesses; reveal resource gaps; improve coordination; practice using the communication network; clarify roles and responsibilities; improve individual performance; improve readiness for a real incident. After personnel are trained, the COOP plan can be tested through one of three types of exercises: Tabletop, Functional and Full-scale (COOP Training).

Tabletop exercises are simulation activities in which a scenario is presented and participants in the exercise respond as if the scenario was actually occurring. New information is presented as the situation unfolds, making the participants reconsider their previous decisions and plan their next actions based on the new information. Typically, a tabletop exercise takes about 2 hours, including the post exercise debriefing (Unit 5).

Functional exercises test a part of COOP activation independent of other responders. This includes testing communications capabilities and equipment; primary and backup infrastructure

systems and services (i.e. emergency power generators); and Recovery of records, critical information systems, services, and data (Unit 6).

Full-scale exercises are as close to reality as possible, testing the organization's total response capability for COOP situations, with personnel deployed and systems and equipment tested (Unit 7). Making the COOP Program an externally inspected program will help convey its importance to commanders/leadership. The best way to highlight the importance of a program/project is to make it one that is inspected and REPORTED by an external agency to the organization's leaders. From that perspective, senior leadership needs to make it an inspection type program with a formal grading system (GO/NO GO, Pass/Fail, etc.) with a similar methodology through subordinate organizational structure.

Considerations

Organizations must be prepared to activate their COOP plans for all emergencies, regardless of warning period, both during regular office hours and non-office hours, including holidays. Activation requires notification of an Emergency Operations Center (EOC), other organizations, as appropriate, and COOP and Non-COOP personnel. Relocation involves the actual movement of MEFs, personnel, records and equipment to the Emergency Relocation Facility (ERF). Relocation also involves transferring communication capability, purchasing supplies and equipment that are not at the ERF, and other planned activities, such as providing network access.

Organizations should plan on having "Go-Kits" to ensure the transition to the ERF occurs smoothly and quickly. These "Go-Kits" are packages of records, information, communication and computer equipment, and other items related to emergency operations. The kits should contain all items that are essential to supporting COOP operations at the ERF (Ready).

While organizations are responsible for the safety and security of their personnel, these personnel are also responsible for the safety and security of their families. Personnel should be encouraged to develop a family disaster plan and to prepare disaster supply kits for their homes, cars, and workplaces. When preparing for emergency situations it's best to think first about the basics of survival; fresh water, food, safety, and warmth (Ready).

Implementation

Implementing COOP plans will be a difficult task that will require that all levels of government accept the understanding that something catastrophic may and will happen again. The federal government has already begun to implement COOP plans for all government agencies. The next step is for all state and local governments to begin preparing their own plans. The federal government should, in the strongest possible way, convince all state and local government agencies to prepare and implement COOP Plans. COOP plans will provide a stronger awareness and preparedness for major issues that will face their communities. The federal government cannot necessarily demand that all levels of government prepare plans; however, they can utilize other methods to persuade them to do so. For instance the federal government should provide grant funding only to COOP - compliant governments.

This may seem to be a harsh method and the tax payers may be the real victims. If state and local governments understand the importance of these plans, everyone will benefit from them. State and local governments should begin with the short term goals which should be accomplished by a set date. This would require manpower and time to begin the goals of short term. Once plans are in place then and only then should state and local governments move forward to the long term goals.

Observation

COOP Plans do not attempt to deal with incidents which are handled routinely by staff and emergency responders. They establish a basis upon which further plans, procedures, guidelines, and agreements can be elaborated. Plans cannot be formulaic or scripted; they cannot anticipate every scenario or foresee every outcome. Therefore, while COOP plans provide guidance, it is understood that it is not intended to replace sound judgment expected to be exercised by those individuals implementing the plan given the circumstances and uncertainties of an emergency.

Conclusion

Homeland security is an ongoing and shared responsibility across the nation. There is an overwhelming number of public and private sector stakeholders that influence the direction of homeland security; all must work together to develop and implement the homeland security strategy by building and maintaining necessary capabilities.

Too many think of COOP as a single operation, such as responding to a hurricane or a flood, and it can be that. For example, the Department of Public Works should have an alternate location for its Emergency Calls Desk so that if the primary location goes out, it can still do the required coordination. Similarly the local police department should have an alternate location should they not be able to e their primary building. That is why the Mission Essential Functions (MEF's) are so important. That is why the primary organization, in order to accomplish its required command and control responsibilities during crisis circumstances, has an alternate Emergency Operations Center.

Should Mary, John and Pete not be available to do X, Y and Z, how would state and local governments continue to operate? If those personnel were assigned to the Work Order Desk and

they weren't available, who else knows how to do those critical coordinating functions? Organizations will need to incorporate a training standard to train three levels down. At times in a hazardous situation a facility is still available and functioning but the people to operate the facility aren't (e.g. sick or taking care of sick family members). State and local governments need to plan for these unforeseen situations. The COOP Plan will identify replacements of key and critical functions.

There are some facilities that can't be duplicated, but then other plans have to be made. If part of the hospital is not available, can the local civilian hospitals support the required tasks? If the fire station is gone, can other surrounding area local fire services support the mission? Can they identify the communications, facilities, and people required (by name). They must be able to identify alternate locations with required communications support and develop cross training three levels down. And for some like me the COOP site is at home with a computer and cell phone.

Each organization should formulate a COOP plan immediately, starting with defining their near term goals of establishing the foundation for a Continuity of Operations planning format and providing clear short term guidance to staff by government priorities. Once the short term goals are completed, they need to move forward with their long term goals of designing a process to test assumptions, create a comprehensive community vision, and translate the Continuity of Operations goals into an implementation plan to guide the course for the future.

References

(1 DHS) Department of Homeland Security. FEMA Continuity of Operations Retrieved from http://www.fema.gov/government/coop/index.shtm

Chertoff, M. (February 2008). Federal continuity directive 2 (fcd 2) federal executive branch mission essential function and primary mission essential function identification and submission process. Retrieved from http://www.fema.gov/pdf/about/offices/fcd2.pdf.

COOP Training: Course Map. Retrieved from http://www.fema.gov/government /coop/index.shtm

Department of Homeland Security Federal Emergency Management Agency. (n.d.). Continuity of operations division. Retrieved from http://www.fema.gov/about/org/ncp/coop/index.shtm

(ESF) Emergency Support Function Annexes: Introduction. Retrieved from www.fema.gov/pdf/emergency/nrf/nrf-esf-intro.pdf

Executive Order 12656 of November 18, 1988. Assignment of Emergency Preparedness Responsibilities Retrieved from http://www.fas.org/irp/offdocs/EO12656.htm

Federal Register Vol. 53, No. 228. Wednesday, November 23, 1988Presidential Documents Executive Order 12656 of November 18, 1988. Retrieved from http://www.fas.org/irp/offdocs/EO12656.htm

(FEMA1) Federal Emergency Management Agency Continuity of Operations (COOP) Multi-Year Strategy and Program Management Plan Template Guide. Retrieved from http://www.fema.gov/pdf/government/coop/MYSPMPTemplateGuide.pdf

(FPC) Federal Emergency Management Agency FPC 65 Retrieved from http://www.fas.org/irp/offdocs/pdd/fpc-65.htm

Hunter, C. (n.d.). BrainyQuote.com. Retrieved March 8, 2012, Retrieved from

BrainyQuote.com Web site:
http://www.brainyquote.com/quotes/quotes/c/charliehun335350.html

(MEF) Mission Essential Functions Template Retrieved from www.ehs.ufl.edu/RiskMgmt/
COOP/COOP_Training.ppt

National Continuity Policy –NSPD NSPD-51/HSPD HSPD-20 Pl March 26, 2008
Association of Contingency Planners Retrieved from
http://www.acpdc.org/presentations/NCP.pdf

PDD-NSC-67 Enduring Constitutional Government and Continuity of Government Operations
21 October 1998 Retrieved from http://www.fas.org/irp/offdocs/pdd/pdd-67.htm

Ready America. Retrieved from http://www.ready.gov/america/getakit/

Unit 5: The Tabletop Exercise. Retrieved from http://www.acp-wa-state.org/meetingsdoc
/october2007/03%20Tabletop%20Exercise%20 Guidelines%20-
20FEMA%20Example.pdf

Unit 6: The Functional Exercise training. Retrieved from
fema.gov/EMIweb/downloads/is139Unit6.doc

Unit 7: The Full-Scale Exercise Retrieved from
training.fema.gov/emiweb/downloads/is139Unit7.doc

Chapter 2

COOP Management Concerns

"Surround yourself with the best people you can find, delegate authority, and don't interfere as long as the policy you've decided upon is being carried out."

Ronald Reagan

"Good management is the art of making problems so interesting and their solutions so constructive that everyone wants to get to work and deal with them."

Paul Hawken, *Natural Capitalism*

In preparing the Management chapter of my Master's project, I had a hard time deciding how to begin this assignment since the homeland security strategy I chose didn't necessarily address a particular organization but addressed Continuity of Operations: planning to ensure mission stability and continuation of essential functions and services across a wide range of potential events. This strategy addresses all governmental organizations large and small. This paper will discuss the six components consistent with the learning outcomes from the (CRJ 602) Management course. The components that will be discussed are management principles; my chosen management model, Core Functions, understanding the essence of individual and group dynamics; Effective Communications; and the Challenges to Management.

I am a retired Marine Corps Gunnery Sergeant with a broad background covering 20 years as a leader, inspector, advisor and trainer in Force Protection, Security and Operations Management. During my career I have interacted on a daily basis with many people, providing information and ensuring my audience had a clear understanding of organizational rules, regulations and guidelines, and ensuring compliance with all applicable regulations. I have

served in positions ranging from front line supervisor to mid-level management. I don't consider myself an expert by any sense of the word, just a well rounded individual. I offer this information as a multiplier for the next phase of my life and as the basis of this chapter of my Master's Project.

Management Principles

The three levels for being a superior manager are human, technical, and conceptual skills; the necessary functions of a manager are planning, organizing, delegating and controlling an organization (The Personal MBA).

Human skill is the power to communicate to fellow co-workers, a skill that 99% of all companies look for in a manager because if you do not possess the ability to correspond with other employees, then you will not succeed in a manager position. You must be a "people person" in order to hold a job as a manager because on a daily basis you will be working with various associates and will need to know how to hold conversations and help your employees. Learning how to communicate effectively with people is a key principle of management that you will need in order to be successful in your position.

Technical skill is the ability to process the technical side of work. Proficiency in the technical knowledge of your job and company is critical if your job requires you to be more "hands on." Many managers find themselves less educated on the technical side of the job than their employees so if they lose their managerial position, they are forced to come to the reality that there are far more people educated in technical work than they are and so may slowly fall down the ladder. In order to not let this happen, you must stay up to date with the technical aspects of your job in order to assure your bosses and your company that you are the right person for the position (Posner, R).

Conceptual skills involve the formulation of ideas and concepts. Managers that have great conceptual skills generally possess the power to create innovative ideas and deliver abstract theories. This form of management will give your company the edge it needs against its competitors if you can formulate groundbreaking concepts for your company that will push them ahead of the competition (WiseGeek).

Managers also have duties no matter what their skill level is; these responsibilities include planning, organizing, directing and controlling. These functions are necessary when working as a manager at any level. You might view your principles of management as the separate skills or the basic duties of a manager. Whichever you hold as the most important, you must also keep in mind that great managers will possess all of these skills and be a vital asset to their companies. A good leader has the ability to get people to follow. It means more than just telling or getting people to do what is asked; a good leader motivates people to want to do what is asked. A good leader must provide a clear vision and a direction.

There are many philosophies of leadership, and advocates of each of them declare their "style" as the most effective: authoritarian, dictatorial, autocratic, and democratic. The list goes on and on. However, in my opinion none of them is right. In order for leadership to be effective it needs to be dynamic. Active leadership is a dual-focused form that is able to be adjusted for use in different conditions and allows leaders to be proactive (Performance). A leader must utilize a fluid style of leadership that he adjusts based on the people he/she is leading and on the circumstances in which they find themselves. A great example of this is in recruit training: recruit and Drill Instructor are different and the method for correcting them is also different as well. Yelling, screaming, and at times, threatening to either drop or recycle them may work well

with one recruit but not with all. In other instances you may have to pull individuals aside and talk to them as if they were your son or daughter. What works for some doesn't work for all.

Leadership in the simplest form is being the one person who leads from the front, makes critical decisions, and ensures that the people who work for you are taken care of. Personally, leadership means responsibility and taking initiative to do the right things. The leader is someone who cares about the means to the end while having the ability to complete a task under any circumstances.

Henri Fayol described management as being a composition of five functions: namely planning, organizing, leading, coordinating and controlling.

Planning involves identification of your business goal and the way to reach it. Leaders use planning to ensure that an approach for reaching goals will be practical. Planning reduces confusion, builds subordinates' confidence in themselves and their organization, and allows flexibility to adjust to changing situations. Smart planning presents a shared understanding and ensures that a mission is accomplished with a minimum of wasted effort. You need to communicate your plan to your employees and accept their feedback (Fayol, H).

Organizing involves the assignment of tasks and allocation of resources throughout the organization. Responsibility and accountability for using available resources effectively and for planning the organizing, directing, coordinating, and controlling of subordinates to accomplish assigned tasks (Fayol). Whether you are starting a new company or improving an existing one, it is important to have a business mission, concept, and vision. Finally, in order to improve, you must have a vision or goal of where you want to end up (Kurtis, R).

Leadership is a management skill in itself; the process involves influencing people by providing purpose, direction, and motivation, while operating to accomplish the mission and

improve the organization. Employees of any organization deserve competent, professional, and ethical leadership. They expect their leaders to respect them as valued members of effective and cohesive organizations. A leader has strong intellect, physical presence, professional competence, high moral character, and serves as a role model. A leader not only dreams but also provides the employees with a framework for the fulfillment of his dreams (Fayol, H).

Coordination and control are important for the success of a business. In all cases, preparation includes detailed coordination with other organizations involved or affected by the operation or project. In any case preparation may include ensuring the necessary facilities and other resources are available to support the assignment**.** Coordination allows leaders to constantly interact and share thoughts, ideas, and priorities through multiple channels, creating a more complete pictures. Dominating the counseling by talking too much, giving unnecessary or inappropriate advice, not truly listening, and projecting personal likes, dislikes, biases, and prejudices all interfere with effective counseling. Competent leaders avoid rash judgments, stereotyping, losing emotional control, inflexible counseling methods, or improper follow-up (Fayol, H).

Management Model

The Department of Homeland Security's (DHS) main goal is to provide the unifying core for the vast national network of organizations and institutions involved in efforts to secure our nation. This is accomplished by bringing together 22 departments covering a wide array of areas under one leadership structure. This department includes everything from the Coast Guard, Transportation Security Administration, Customs and Border Patrol, Immigration, FEMA, and the Secret Service, among others (DHS).

The Department of Homeland Security was instituted to correct the coordination problems that surfaced in the aftermath of the 9/11 terrorist attacks. Even after 5 years of efforts at building new coordination mechanisms and new organizational priorities, DHS and FEMA were faulted for their response to Hurricane Katrina. Again, there were issues of jurisdiction, inability to communicate across agencies and level of government, and lack of quick response (Volkomer,). A new agency with unchallenged jurisdiction was created by the Congress and signed into law by President Bush.

The management model I chose is the Divisionalized Form. Each model presents various challenges; however I do believe this one would work best. One key issue or challenge with this model is that "Headquarters wants tighter oversight while divisional managers try to evade corporate controls." Another example identified as an issue is that "headquarters may lose touch with operations." A simple solution is getting out and visiting your divisions. Set up a disciplined approach that gets you out from behind your desk. It is amazing the effect you can make walking around, asking questions, and correcting deficiencies when required. This is the obvious leadership approach everyone talks about but rarely does.

Every organization requires the making of decisions, the coordinating of activities, the handling of people, and the evaluation of performance directed toward group objectives. There are many different ways to gather information for assessment purposes. The Myers-Briggs Type Indicator (MBTI) assessment uses four dimensions of personality to identify 16 different personality types. Although I agree this tool could be helpful to managers, I don't think it is the end-all tool. The document mentions "gut feeling" and this to me is just as important as a chart that someone has come up with (Huitt, W).

The ability to assess a situation accurately and reliably against desired outcomes, established values, and ethical standards is a critical tool for leaders to achieve consistent results and success. Assessment occurs continually during planning, preparation, and execution; it is not solely an after the fact evaluation. Accurate assessments require instinct and intuition based on experience and learning. It also demands a feel for the dependability and soundness of information and its sources. Periodic assessment is necessary to determine organizational weaknesses and prevent mishaps. Determining causes, developing subordinate leadership, and initiating improvements are essential to management (Robbins, S).

A manager who participates in normal functions, but not micromanaging, is able to identify each member's strengths and work out a plan in which he is able to capitalize on each one's strengths without making any single member feel less productive or left out. Working with teams will ensure that each team understands its objectives and aims to ensure it fulfills its requirements.

Core Functions

Core Functions will vary from organization to organization whether large or small. The Department of Homeland Security has published numerous documents referring to Mission Essential Functions (MEF's). Although these MEF's are in official Homeland Security documents, they can be tailored to meet the Core Functions of any sized organizations.

In July 2005, then Secretary Chertoff presented a six-point agenda for the Department of Homeland Security "to deal with the potential threats, both present and future that face our nation" : increase overall preparedness, particularly for catastrophic events; create better transportation security systems to move people and cargo more securely and efficiently; strengthen border security and interior enforcement and reform immigration processes; enhance

information sharing with our partners; improve DHS financial management, human resource development, procurement and information technology; realign the DHS organization to maximize mission performance (Six Point).

You cannot teach someone to adapt in a chaotic situation. The military calls this "Fog of War," a term used to describe the level of uncertainty in situational awareness experienced by participants in operations. Many leaders have tried to replicate a chaotic situation during training but one thing is certain, you are going home at the end of the exercise. Training exercises whether military or civilian can be a good starting point especially when you add stress and realism to them. If they are just doing a paper drill subordinates will be lackadaisical. The realism will test their will power, judgment, and loyalty.

As an infantry platoon sergeant I have been in situations where we didn't know what we were facing. Landing somewhere on potential enemy soil places doubt in your mind. However if you have trained and exercised to your utmost capability, this eases the tension slightly. Also as the leader you cannot show fear; you must present yourself as very confident. If it appears you are not confident or you show fear, everyone else will do the same. If you ever ask service members why they did well in combat, it's not because they were superstars, rather it was the fear of letting their buddies and unit down.

Purpose provides what the leader wants done, while motivation and inspiration provide the energizing force to see that the purpose is addressed and has the strength to mobilize and sustain effort to get the job done. Motivation and inspiration address the needs of the individual and team. Indirect needs like job satisfaction, sense of accomplishment, group belonging, and pride typically have broader reaching effects than formal rewards and punishment.

Individual and Group Dynamics

Most leaders are also subordinates within the framework of organizations or institutions. All members of the organization are part of a larger team. A technical supervisor leading several specialists is not just the leader of that group. That team chief also works for someone else and that team has a place in a larger organization. Part of being a responsible subordinate implies supporting the chain of command and making sure that the team supports the larger organization and its purpose. The team chief knows that when the team makes a mistake or falls behind in its work, there is an obligation to try making it succeed, even if the chief initially has doubts that it will. If everyone in the organization understands their requirements and roles, it shouldn't matter if it's normal day-to-day routines or a major event.

When considering Individual Differences we need to remember that people in general have a strong desire to be accepted by a group throughout life. This acceptance gives the assurance of support and comfort from others who are alike. People in such groups have set beliefs which cause them to ignore differences in their surroundings. The strength in organizations provokes fear in those who want to express their individual differences. Those wanting to be different are afraid of the judgmental ridicule they will face from their fellow group members. Affiliation in a group gives people encouragement, friendship, and comfort as long as the affiliation continues to have the same general understanding as the rest of the group.

Leaders are here for a reason. Good leader will teach you everything they have learned from their experiences. There is truly no knowledge that is not power. Sometimes we miss the most important lessons when we do not know when to close our mouths and open our ears. Learning how to be a good follower means being open minded and knowing how to take direction from supervisors. Learning how to follow orders is like fitting gloves on a future leader. Honing your listening skills is a key factor in the makings of a good follower. Then by

understanding how to hear and comprehend the tasks placed on you by your leaders, you will know how to communicate with your own employees when the time comes.

Duty extends beyond everything required by law, regulation, and orders. Professionals work not just to meet the minimum standard, but consistently strive to do their very best. Leaders commit to excellence in all aspects of their professional responsibility.

Employees may feel they have no voice within their organization, especially if they do not hold a management position. But every action you make is a reflection of your managers' and your own leadership skills. Being able to carry out any responsibility given to you, no matter how simple or daunting, shows a great deal about your dedication and also shows what you have learned from your leaders.

Effective Communications

Leadership that gets results depends on good communication. Although communication is usually viewed as a process of providing information, communication as a skill must ensure that there is more than the simple transmission of information. Communication needs to achieve an understanding and must create new or better awareness. Communicating critical information in a clear manner is an important skill to reach a collective understanding of issues and solutions. It is passing on thoughts, presenting recommendations, bridging sensitivities and reaching a general consensus. Simply put, leaders cannot lead, supervise, build teams, counsel, or mentor without the ability to communicate clearly.

An important form of two-way communication to reach a shared understanding is active listening. Although the most important purpose of listening is to understand the thoughts of whoever is speaking, listeners should provide an occasional signal to the speaker that they are still attentive. Active listening involves avoiding interruption and keeping mental or written

notes of important points or items for clarification. Good listeners will be aware of the content of the message, but also the importance and emotion of how it is spoken. It is important to remain aware of barriers to listening. Do not formulate a response while it prevents hearing what the other person is saying. Do not allow distraction by anger, disagreement with the speaker, or other things that can hold up the process (The Art).

Frequently, leaders communicate more effectively with informal networks than directly with superiors. Sometimes that produces the desired results but can lead to misunderstandings and false judgments. To run an effective organization and achieve mission accomplishment without excessive conflict, leaders must figure out how to reach their superiors when necessary and to build a relationship of mutual trust. First, leaders must assess how the boss communicates and how information is received. Some use direct and personal contact while others may be more comfortable with weekly meetings, electronic mail, or memoranda. Knowing the boss's intent, priorities, and thought processes enhance organizational effectiveness and success. A leader who communicates well with superiors minimizes friction and improves the overall organizational climate.

To prepare organizations for unavoidable communication challenges, leaders need to create training situations in which they are forced to act with minimum guidance or only the leader's intent or vision. Leaders provide formal or informal feedback to highlight the things subordinates did well, what they could have done better, and what they should do differently next time to improve information sharing and processing. Open communication does more than share information. It shows that leaders care about those they work with. Competent and confident leaders encourage open dialogue, listen actively to all perspectives, and ensure that others can voice up-front and honest opinions, without fear of negative consequences.

The first step in problem solving is recognizing and defining the problem. This step is crucial, as the actual problem may not be obvious up front. As a result, leaders determine what the problem is by clearly defining its scope and limitations. Leaders should allow sufficient time and energy to define the problem clearly before moving on to other steps of the problem-solving process. A problem exists when there is a difference between the current state or condition and a desired state or condition. Leaders identify problems from a variety of sources. These include: directives or guidance, decision maker guidance, subordinates, and personal observations.

There are numerous problem-solving techniques; creative problem solving which involves everyone concerned with the problem can encourage many types of creative thinking such as brainstorming, group solutions, and other techniques that might not have been considered. One key to creative problem solving is thinking "outside the box," which means thinking outside the confines of what is normal or accepted. Some would say that problem solving commonly means thinking in innovative ways without the usual structure; this is how most creative problem solving is truly accomplished.

The Challenges to Management

A major concern for those managing any organization as it should be managed will always be to motivate their employees in an effort to reach their goal as cost effective and as quickly as possible. Motivation is difficult to explain as well as practice. However, motivation is still the one thing that makes people productive in their jobs. The motivated employee learns fast, deals with customers courteously and efficiently, is cooperative with other employees, and is committed to helping achieve the kind of results your organization needs. Unfortunately, these types of employees do not grow on trees, and must be assisted to become truly motivated towards an organization's goals.

If some are not performing as they should, don't discipline or counsel them in public, but take them aside and tell them their performance is lacking and they need to correct their deficiency. Public reprimand is unprofessional, and the negativity lowers the morale of the workforce. On the other hand if an employee performs above expectations, recognize them publicly. This recognition could be in the form of a simple "job well done," some sort of certificate, or maybe even a day off. Recognition in forms other than monetary compensation provides employees a sense of satisfaction and belonging. Creating a culture of encouraged initiative will create greater results than an environment of competition between employees. Currently times are hard and one thing that many Americans haven't experienced yet is not having a job. The mere possibility of losing your livelihood is all the motivation you should need to be the best employee and keep your job.

Some of the factors that were discussed include the concept of employees as partners, motivating employees, what makes people tick, and harmony in the workplace. Employees who participate in their organization's decision-making processes and who feel that they have a voice in the company have a higher job satisfaction. Employees who work for any organization may have the ideas to take an organization to its limits, so all they need is a good way to open up the communications channel. Senior leadership and managers need to link the communications gap between those who make decisions and those who execute them, so a stronger and more effective team environment will result throughout the organization.

Being a good manager is taking care of your people. Being a good manager is having strong moral and physical courage (Perry, J). Being a good manager is standing up for your employees and supporting them, even if it's not a popular decision with your superiors.

Sometimes you have to punish, praise, and maybe provide a shoulder to cry on. But if you take care of your employees, they will take care of doing the mission at hand.

References

The Art and Science of Problem Solving. Retrieved from http://192.197.62.35/courses/ctec1335/docs/ProblemSolving.pdf

Fayol, Henri. Fourteen principles of management Retrieved from http://www.provenmodels.com/4

Posner, Roy Growth. Perfect Skills Accomplishes http://www.gurusoftware.com/gurunet/personal/topics/Skills.htm

What Are Conceptual Skills? Retrieved from http://www.wisegeek.com/what-are-conceptual-skills.htm

Kurtis, Ron. Organizing Your Business http://www.school-for-champions.com/business/organize.htm

The Personal MBA. Do You Have These Core Human Skills? http://personalmba.com/core-human-skills/

Huitt, William G, David A. DeCenzo, Problem Solving and Decision Making: Consideration of Individual Differences Using the Myers-Briggs Type Indicator

Robbins, Stephen P, David A. DeCenzo. The fundamentals of leadership; essential concepts and applications.

Department of Homeland Security. http://www.dhs.gov/index.shtm

Walter E. American Government, 10th ed. Upper Saddle River, NJ: Prentice Hall, 2003

Birkland, Thomas A. Disasters, Catastrophes, and Policy Failure in the Homeland Security Era

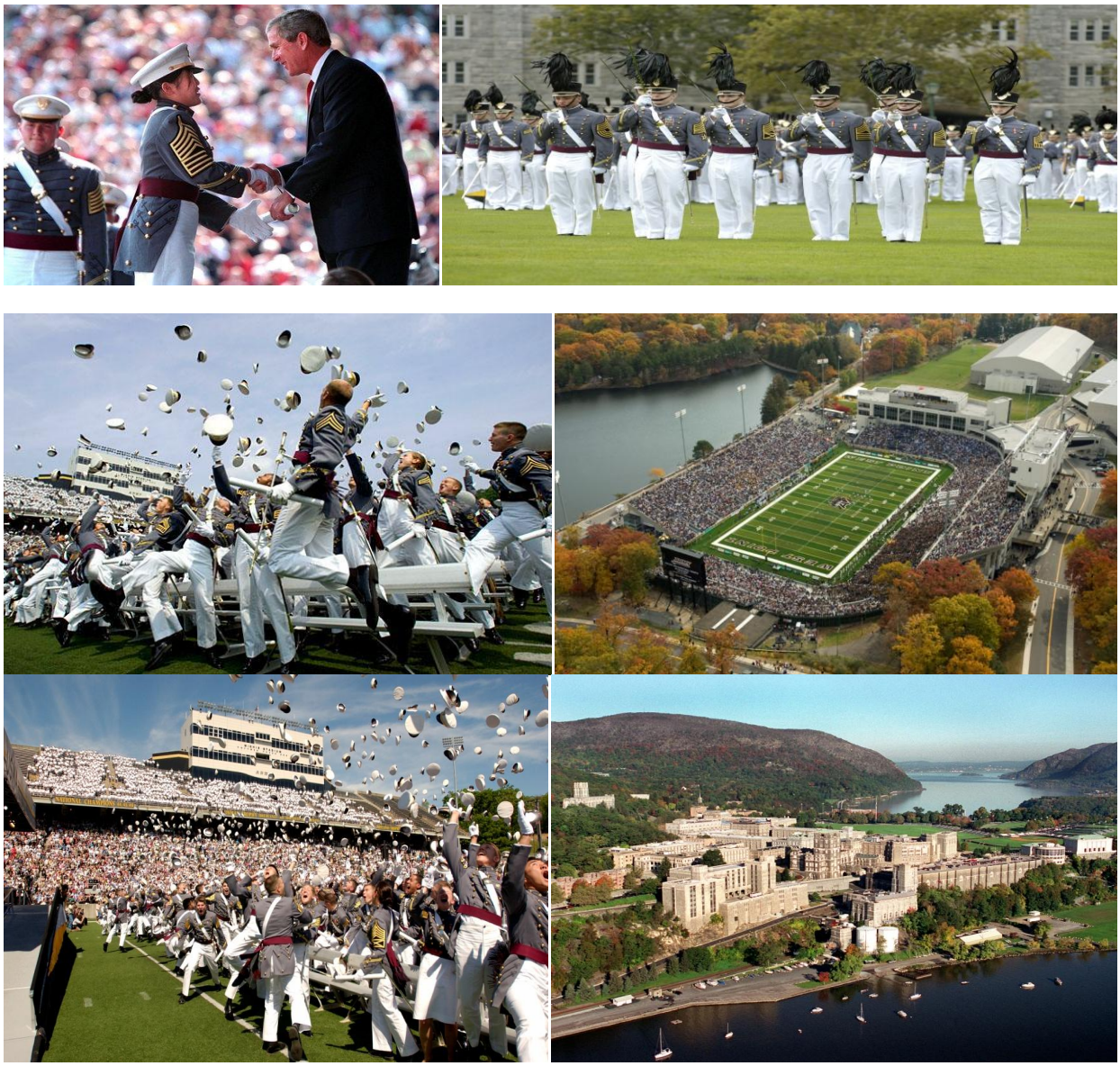
(Six Point). Department of Homeland Security. Department Six-point Agenda. Retrieved from http://www.dhs.gov/xabout/history/editorial_0646.shtm

Perry, James L., Debra Mersch, Laurie, Pearlburg. Motivating Employees in a New Governance

Era: The Performance Paradigm Revisited.

Chapter 3

Antiterrorism Strategic Plan



February 2011

United States Military Academy at West Point, Senior Commander Executive Summary

EVENT: Brief of West Point Antiterrorism Strategic Plan to the Senior Commander

Date: TBD

Time: TBD

Location**:** Senior Commander's Conference Room

Purpose of Event: To brief the Senior Commander on the West Point Antiterrorism Strategic Plan (Draft) in order to outline the goals and objectives to improve the Antiterrorism program services for all personnel of the United States Military Academy at West Point over the next four years.

Parties Involved**:**

Mr. Peddy	Director, DPTMS
Mr. Cassidy	Installation ATO
Col. Tarsa	Garrison Commander
Lt. Col. Hawes	Provost Marshal
Col. Stafford	Chief of Staff
Brig. Gen. Rapp	Commandant of Cadets
Brig. Gen. Trainor	Dean of the Academic Board

Goals and Objectives:

Strategic Goal #1: Implement effective AT risk management processes and ensure the timely and pertinent dissemination of AT threat information and intelligence.

Strategic Goal #2: Develop and execute proactive, relevant and viable AT plans and AT Program management.

Strategic goal #3: Conduct effective AT training and execute realistic AT exercises.

Strategic goal #4: Optimize the planning, programming and execution of resources, including research, development, test and evaluation (RDT&E) in support of AT programs.

Strategic goal #5: Execute holistic, comprehensive reviews of AT programs to ensure compliance with ARNORTH AT Program standards.

Conclusion. This is the first iteration of the West Point Antiterrorism Strategic Plan and builds directly on the ARNORTH AT Strategic Plan. It reflects an increased understanding of the terrorist threat, progress of previous strategic initiatives and complements Army and DoD intent in the larger scope. It implements goals and objectives to refine and energize continued improvement of the Army Antiterrorism program. It delineates areas of emphasis and by so doing sets priorities designed to close "gaps and seams" and provoke further progress. Moreover, the goals and objectives give direction for distribution of resources and address risks while sustaining progress.

Related Materials: Draft of West Point Antiterrorism Strategic Plan

6. POC: Matt Cassidy, installation Antiterrorism Officer, X3650

This strategy represents a course of action to direct our improvements over the next few years. It governs the application of resources and balances risk against necessity by providing enduring goals and objectives that encourage initiative at all levels. Through continual evaluation this plan must remain ahead of the threat evolution and retain the flexibility necessary to react to unforeseen circumstances.

Building a formidable antiterrorism program takes time; nevertheless, time must be balanced with a sense of urgency. We need to close our remaining gaps. The West Point Antiterrorism Strategic Plan charts the path for the next phase of actions. It calls for substantial improvement in antiterrorism in every facet of operations. We cannot prepare for long-term success unless we have embedded antiterrorism in training, leader development and education. We must educate and train leaders, from strategic to tactical, for their role in preventing terrorist attacks. That level of awareness and vigilance is our most certain defense. Building an effective evaluation and reporting system is the next priority. We know our missions, our operations, and our responsibilities. Are we prepared for terrorists focused on disruption and destruction? An effective system of assessments, reporting and continuous improvement will provide the feedback loop we need so Commanders can manage risk appropriately.

There are four reasons for this Antiterrorism Strategic Plan: It guides all West Point elements toward improved antiterrorism; it supports Army Title 10 missions and Transformation; it sets priorities for the Army Antiterrorism Program; it supports National and DOD strategic goals. This Strategic Plan will be explained through the overview and the West Point plan for the goals, performance objectives, and milestones.

CHAPTER 1 – STRATEGIC PLAN OVERVIEW

1. PURPOSE. This Strategic Plan, issued in compliance with reference (j), will guide the West Point Antiterrorism (AT) Program by articulating ARNORTH AT strategic goals and performance objectives, and by providing a construct to implement, measure, and report on their accomplishment. This plan serves as guidance for all West Point activities.

2. BACKGROUND. The West Point AT program is a collective, proactive effort focused on the prevention and detection of terrorist attacks against Army personnel and their families, selected Army contractors, facilities, units, installations, and infrastructure critical to mission accomplishment. It focuses on the planning and preparation required defending against, and responding to, terrorist incidents. The West Point AT program supports the ARNORTH and DoD goals of deterring threats and coercion against U.S. interests, defeating global terrorism, and transforming the DoD to meet the challenges and requirements of the 21st Century.

3. AT VISION. West Point accepts as reality the intent of those that would use terrorism as a tool to destroy people, disrupt our mission, and distract us from our responsibilities. West Point acknowledges that it is a symbolic representation of both the nation and the United States Army. As such, the installation, and the Corps of Cadets in particular, present a lucrative target for terrorists who wish to strike against the United States. West Point will protect the Corps of Cadets and its staff and faculty, and train the cadets as future Army leaders to think and operate in an environment where the potential for terrorism exists. In addition to training future Army leaders, West Point will host a center of excellence, dedicated to the study of combating terrorism, which serves as a source of knowledge for current and future Army leaders.

4. AT MISSION. West Point conducts force protection and law enforcement operations to protect the Corps of Cadets, the West Point Community, and visitors by deterring, denying and defending against enemy attacks. On order, implements contingency plans to mitigate or respond to criminal or terrorist activities directed against personnel or property on West Point.

5. INTENT. The intent of the West Point AT Strategic Plan is as follows:

Integrate actions designed to prevent terrorist attacks

Support ARNORTH AT Strategic Plans

Embed AT concepts throughout the Academy and West Point military reservation.

Host a Center for Combating Terrorism

Incorporate a terrorist environment in cadet military training

Add academic courses related to the study of insurgency and terrorism

Demand active leader participation in the AT program

Prioritize AT efforts over the long term

Endeavor to anticipate the future environment

Establish a system to review and adjust the West Point AT Strategic Plan over time

6. CONCEPT. The West Point AT program focuses on supporting the ARNORTH Strategic Plan and Goals. The ARNORTH AT Program has seven (7) strategic goals, listed below, and thirty-nine (39) supporting performance objectives to facilitate progress toward achieving the stated vision and satisfying the intent of reducing vulnerabilities to terrorist acts. Since the West Point AT strategy supports the Army AT strategy, some goals and performance objectives listed in this plan will maintain a numbering convention consistent with ref (a). The goals are desired outcomes with expected attainment ranging from one to four years. The performance objectives

listed for each strategic goal are intended to contribute to achieving the AT strategic goals by stating in clear, measurable terms the target level of performance expected for each objective.

STRATEGIC GOAL #1: Implement effective AT risk management processes and ensure the timely and pertinent dissemination of AT threat information and intelligence.

STRATEGIC GOAL #2: Develop and execute proactive, relevant, and viable AT plans and AT Program management.

STRATEGIC GOAL #3: Conduct effective AT training and execute realistic AT exercises.

STRATEGIC GOAL #4: Optimize the planning, programming, and execution of resources, including Research, Development, Test, and Evaluation (RDT&E) in support of AT programs.

STRATEGIC GOAL #5: Execute holistic, comprehensive reviews of AT programs to ensure compliance with ARNORTH AT Program standards.

STRATEGIC GOAL #6: Develop a reporting and evaluation system that provides effective and timely data sufficient to apply resources and adjust the program to fit a changing environment.

STRATEGIC GOAL #7: Embed AT concepts throughout the IMA by developing, implementing, and sustaining AT training and doctrine for Army military and civilians.

The AT Branch, ARNORTH provided an estimate of each of the performance objectives to establish the Army baseline (current attainment in terms of percentages), so that appropriate milestones (attainment in terms of percentages over the years ahead) could be developed in order to meet the DoD timeline mandates. The Army baselines are estimates only, generated to provide a start point for evaluating the progressive nature of the Strategic Plan. Substantial measures of success are included in each performance objective. In all cases, the most effective evaluation of our AT posture will become apparent over the course of the Strategic Plan rather than a single year.

7. RESPONSIBILITIES.

a. Installation Commander.

(1) Serve as the West Point Force Protection Officer.

(2) Establish an Antiterrorism Executive Committee (ATEC). The membership include the Superintendent, the West Point Chief of Staff, G3, the Garrison Commander, the West Point counterintelligence Coordinating Authority, the Commandant, the Dean of the Academic Board, and the Director of Plans, Training, Mobilization and Security (DPTMS).

(3) Establish an Antiterrorism Working Group (ATWG). The membership will consist of a representative from each of the major activities and tenant military units.

(4) Ensure force protection is aggressively managed in compliance with DoD, NORTHCOM and ARNORTH regulations and guidance.

(5) Provide guidance and oversight concerning force protection matters.

b. Commandant

(1) Embed antiterrorism concepts into realistic cadet field training.

(2) Leverage the operational experiences of your staff and faculty to provide cadets with a field training and academic environment for the study of terrorism and counter-terrorism.

(3) Support the annual West Point antiterrorism exercise.

(4) Serve as a member of the Antiterrorism Executive Committee.

c. Dean of the Academic Board.

(1) Support the global war on terror through education, research and policy analysis.

(2) Leverage the operational and academic expertise of our staff and faculty to provide cadets with experiential opportunities for studying terrorism and counter-terrorism.

(3) Develop and sustain a Center for Combating Terrorism that will develop, teach, and support academic courses related to the study of insurgency and terrorism.

(4) Conduct research and policy analysis so that the Academy and the Army can endeavor to anticipate the future environment with respect to terrorism.

(5) Support the annual West Point antiterrorism exercise.

(6) Serve as a member of the Antiterrorism Executive Committee.

d. Garrison Commander.

(1) Serve as a member on the Antiterrorism Executive Committee.

(2) Chair the Antiterrorism Working Group.

(3) Execute the West Point antiterrorism plan

(4) Support the West Point antiterrorism exercise.

e. Director, Plans, Training, Mobilization and Security.

(1) Provide operational oversight, coordination and technical guidance for the West Point antiterrorism plan.

(2) Chair the Antiterrorism working group meeting at least quarterly to review and assess West Point's progress in achieving the stated performance objectives of this Strategic Plan.

(3) Host the semi-annual Antiterrorism executive committee.

(4) Report status of all AT strategic goals and performance objectives of this plan to ARNORTH annually, as directed.

(5) Plan, coordinate and execute the annual West Point antiterrorism exercise.

(6) Serve as a member of the Antiterrorism Executive Committee.

f. G-3.

(1) Provide intelligence input to the quarterly West Point threat working group.

(2) Develop and publish the annual West Point terrorist threat assessment.

(3) Direct the annual West Point Antiterrorism exercise.

(4) Serve as a member of the Antiterrorism Executive Committee.

g. Directors of Major Activity Directorates & Commanders of tenant units.

(1) Review the strategic goals, performance objectives, and expected levels of performance contained in Chapter 2.

(2) Increase awareness and develop procedures as appropriate.

(3) Implement sound training and exercise programs to increase awareness and proficiency and to reduce the potential for a terrorist attack in areas of responsibility.

(4) Provide a representative to the West Point ATWG and report on progress towards achieving the stated AT strategic goals and performance objectives of this plan.

8. EVALUATION. The primary method to determine attainment of AT strategic goals, performance objectives, and milestones of this plan will be via internal West Point AT Program assessments, the Joint Service Integrated Vulnerability Assessment (JSIVA), Higher Headquarters Assessments (HHA), Organizational Inspection Program (OIP), and Army Inspector General Audits. Additionally, the monthly ATWG meetings, chaired by the DPTMS, will serve as a venue to review attainment of AT strategic goals and performance objectives. The Core Vulnerability Assessment Management Program (CVAMP) will be the database used to store and retrieve these performance objectives parameters. At this time, ref (d) at Appendix A requires all VA results be recorded in CVAMP within 120 days of the assessment. When appropriately modified, CVAMP will also record the annual compliance with ref (a), and therefore, generate required annual reports.

9. IMPLEMENTATION. This AT Strategic Plan is effective immediately.

CHAPTER 2 – WEST POINT PLAN FOR IMPLEMENTING ARNORTH AT STRATEGIC GOALS, PERFORMANCE OBJECTIVES, AND MILESTONES

1. This chapter describes the strategic goals and performance objectives and each table includes the following:

a. Performance Objective: Description of performance objective.

b. Applies to: Depicts level of command oversight for performance objective.

c. Army Baseline: The baseline performance indicator serves to establish the frame of reference by which actual achievement shall be compared.

d. Acceptable Performance: Depicts performance goals, in terms of percentages, over a range of future years.

e. Measure of Performance: How the performance will be measured.

f. Discussion: Amplifications/Reference.

Performance Objectives and Performance Milestones. The performance indicators listed below contribute to achieving the AT strategic goals by stating specific objectives, measurable terms and target level of performance expected for each performance objective. Although the baseline and subsequent targets are both estimates and subjective evaluations, they serve to guide efforts toward the end goal. Through assessments and reporting, West Point activities can track the progress to the assigned performance objectives.

2. Strategic Goal #1: Implement effective AT risk management processes and ensure the timely and pertinent dissemination of AT threat information and intelligence. This goal contains seven West Point supporting performance objectives.

a. Performance Objective 1A: Threat/Local Observation Notice (GUARDIAN) Reporting.

Performance Objective	- Ensure West Point garrison implements Threat and Local Observation Notice (GUARDIAN Reports) reporting. - Ensure s West Point AT Plan incorporates GUARDIAN reporting procedures.
Applies to	Directorate of Emergency Services (DES), Directorate of Plans, Training, Mobilization and Security (DPTMS)
Army Baseline	50%.
ARNORTH Acceptable Performance	100% by the end of FY11.
West Point Acceptable performance	100% by end of FY11.
Measure of Performance	AT plan incorporates GUARDIAN Reporting.
Discussion	Reference: Dep. Sec. Def Memo dated 13 Sep 2007, DoD and ARNORTH plans
Budget/ Resources	There is no additional cost to implement this goal; it is calculated in the ATO salary.

b. Performance Objective 1B: Threat Working Groups (TWG).

Performance Objective	- Ensure West Point activities participate in a TWG at the installation level. - Meets at least quarterly. Increase frequency as required. - Develop and refine terrorism threat assessments. Coordinate and disseminate threat warnings, reports, and summaries to optimize regional situational awareness. - Ensure TWG membership includes, at a minimum, the ATO; the Garrison Commander (or a designated representative); the Directorate of Operations, Plans and Security (G-3) intelligence officer; DES; DPTMS; United States Corps of Cadets (USCC); office of the Dean (Dean); Directorate of Intercollegiate Athletics (ODIA); Keller Army Community Hospital (KACH); Criminal Investigation Command (CID). - Ensure AT plans contain the TWG charter to include: the organization that is hosting if not a Garrison, membership composition, defined responsibilities, and frequency of meetings. - Ensure DPTMS maintains TWG meeting minutes (properly classified) for a minimum of one year.
Applies to	G-3, DPTMS, DES, USCC, Dean, CID, ODIA, KACH
Army Baseline	50-60%.

ARNORTH Acceptable Performance	100% by the end of FY12.
West Point Acceptable Performance	100% by the end of FY12
Measure of Performance	TWG charter incorporated in West Point AT Plan; TWG meeting quarterly as scheduled.
Discussion	Reference: AR 525-13 dated Sept 11. 2008, Critical Task 2; DODI 2000.16 Stnd 8.
Budget/Resources	There is no additional cost to implement this goal, the strategy costs are calculated in the salaries of the member's assigned. The resource impact however is removing some members from their primary responsibilities to perform their TWG functions.

c. Performance Objective 1C: Does not pertain to West Point.

d. Performance Objective 1D: High Risk Personnel (HRP) does not pertain to West Point.

e. Performance Objective 1E. Threat Assessments (TA).

Performance Objective	- Ensure West Point has a comprehensive Threat Assessment (TA) process. - Ensure TAs are conducted annually or more frequently as the terrorist threat environment dictates. - Identify the full range of known or estimated terrorist threat capabilities. - Prepare specific TAs to support operational planning and risk decisions for unique mission requirements or special events. - Ensure reference TA procedures is in our AT plan.
Applies to	G-3, DPTMS
Army Baseline	50-60%.
ARNORTH acceptable performance	95-100% by end of FY11.
West Point Acceptable Performance	G-3 prepares comprehensive annual TA; Intelligence annex to OPORD's prepared prior to special events such as graduation, home football season, Army-Navy Game; specific updates 30 days prior to special events.
Measure of Performance	TA procedures in West Point AT Plan; annual TA prepared and issued by G-3; specific updates 30 days prior to special events.

Discussion	Reference: AR 525-13, Critical Task 2; DODI 2000.16 Stnd 8.
Budget/Resources	The MEVA is not stationary, when the MEVA moves in mass from West Point to various venues in the United States (Philadelphia, Baltimore, College Station, Texas, and Cleveland OH) assessments are required in accordance with DoD standard 6. Standard #6 states; any event or activity determined to be a special security event or other activity involving a mass gathering of >300 DoD personnel The Army/Navy football game is a very high visibility target of national interest, and likewise related events have the potential to be targets for terrorist attacks. The ATO serves as the primary point of contact/liaison between Federal, State, local law enforcement, and emergency services, with officials, and senior leadership. This requirement is to ensure that a Pre-deployment Assessment, Vulnerability Assessment, and Special Event Assessment are conducted as well as route, hotel, Food and Water VA, as well as the venue vulnerability assessment. Additionally coordinating and liaising with a multitude of law enforcement both state and federal as well as civil support agencies. These assessments identify areas of improvement to with stand, mitigate, or deter acts of violence or terrorism. FY11- $3.7K FY12 - $4K FY13 - $4.5K FY14 - $4.6K Max per diem rate for Alexandria, Virginia, Lodging 209, M&IE 49 ($258.00) multiplied by 7 days = Per Diem x days x personnel x trips = $1806.00, Per Diem 7 days @ $258 a day x 2 personnel = $3612.00 is total Travel cost.

f. Performance Objective 1F: Criticality Assessments (CA).

Performance Objective	- Ensure West Point activities implement and conduct at all levels programmatic and procedural actions to protect critical assets (personnel, property, equipment, activities, operations, information, facilities, services, and resources) essential to Army operations. - Ensure DPTMS conducts comprehensive annual Terrorism Criticality Assessments (CA). - Require DPTMS to address and reference CA procedures in the AT plan.
Applies to	DPTMS, DES, DPW, ATWG
Army Baseline	40-60%. by end of FY11
ARNORTH acceptable performance	95-100% by end of FY12.

West Point Acceptable Performance	100% by the end of FY12.
Measure of Performance	West Point AT Plan incorporates CA procedures; ATWG conducts annual CA; CA results briefed to Antiterrorism Executive Committee (ATEC).
Discussion	Reference: AR 525-13, Critical Task 3; DOD I 2000.16 Stnd 5; DODO 2000.12H
Budget/Resources	There is no additional cost to implement this goal; it is calculated in the ATO salary

g. Performance Objective 1G: Vulnerability Assessments (VA).

Performance Objective	- Ensure West Point activities implement, enhance, and conduct at all levels programmatic and procedural actions to determine susceptibility of personnel, assets, and infrastructure to terrorist acts. - Conduct comprehensive annual Vulnerability Assessments. - Require DPTMS to address and reference VA procedures in the AT plan.
Applies to	West Point activities
Army Baseline	10-20%.
ARNORTH acceptable performance	95-100% by end of FY12.
West Point Acceptable Performance	80% VA of critical facilities by the end of FY11, 90-100% of the installation by the end of FY12.
Measure of Performance	2010 AT plan incorporates VA procedures; trained VA team comprised of DPTMS and DES, DPW, DOIM, and DOL members; VA's scheduled for special events.
Discussion	Reference: AR 525-13, Critical Task 3; DOD I 2000.16 Stnd 6 and 16, DOD O 2000.12-H
Budget/Resources	There is no additional cost to implement this goal; it is calculated in the ATO salary

h. Performance Objective 1H: Risk Assessments (RA).

Performance Objective	- Ensure West Point activities implement and/or enhance programmatic and procedural actions to assess and incorporate TA, CA, and VA to attain a comprehensive Risk Assessment. - Ensure DPTMS conducts comprehensive annual RA, and RA for special events. - Reference RA procedures in the AT plan.

Applies to	West Point activities
Army Baseline	10-20%.
ARNORTH acceptable performance	90% by end of FY12
West Point Acceptable Performance	100% by the end of FY13.
Measure of Performance	West Point AT plan incorporates risk assessment; DPTMS conducts comprehensive annual risk assessment for special events.
Discussion	Reference: 525-13, Critical Task 3; DOD I 2000.16 Stnds 15 and 16, DOD O 2000.12-H
Budget/Resources	There is no additional cost to implement this goal; it is calculated in the ATO salary

i. Performance Objective 1I: ATO SIPRNET Access.

Performance Objective	- Ensure designated ATO's assigned or attached have dedicated SIPRNET access. (note: IMCOM objective is dedicated access at the ATO's desk)
Applies to	West Point and Installation ATO
Army Baseline	30-40%.
ARNORTH acceptable performance	90-100% by end of FY10.
West Point Acceptable Performance	Installation ATO with SIPRNET access by end of FY10; dedicated SIPRNET access to ATO's by end of FY12.
Measure of Performance	Percentage of designated ATO assigned or attached that have dedicated access to SIPRNET.
Discussion	Reference: DoD O-2000.12-P, Performance Objective 1I; DOD I 2000.12-H. ATOs require SIPRNET access in order to receive the latest threat information and reference material.
Budget/Resources	Installation of SIPERNET capability and SIPERNET computer lifecycle FY12- $14K FY13 - $4K FY14 - $4K FY15 - $4K

3. Strategic Goal #2: Develop and execute proactive, relevant, and viable AT plans and AT Program Management practices. This goal contains eight West Point supporting performance objectives listed below:

a. Performance Objective 2A: Antiterrorism Working Groups (ATWG).

Performance Objective	- Ensure West Point establishes a standardized Antiterrorism Working Group (ATWG) that meets at least quarterly. - Require DPTMS to develop ATWG charter. - Require DPTMS to reference ATWG charter in the AT plan.
Applies to	West Point and USAG representatives
Army Baseline	60-70%.
ARNORTH acceptable performance	100% by end of FY09.
Acceptable Performance	100% by the end of FY10 **(*note, AT Operation Plan was signed Dec '09)**
Measure of Performance	ATWG comprised of West Point and Garrison activity representatives meeting at least quarterly; charter approved and incorporated in 2010 AT Plan.
Discussion	Reference: AR 525-13, Critical Task 1; DOD I 2000.16 Stnd 10
Budget/Resources	There is no additional cost to implement this goal; the strategy costs are calculated in the salaries of the member's assigned. The resource impact however is removing some members from their primary responsibilities to perform their ATWG functions.

b. Performance Objective 2B: Antiterrorism Executive Committees (ATEC).

Performance Objective	- Ensure West Point establishes an Antiterrorism Executive Committee (ATEC). - Ensure ATEC meets at least semi-annually. - Define ATEC Charter. - Act upon recommendations of the ATWG and TWG to determine resource allocation priorities to mitigate or eliminate terrorism-related vulnerabilities. - Require DPTMS to maintain committee-meeting documentation (action items).

Applies to	West Point
Army Baseline	70-80%
ARNORTH acceptable performance	100% by end of FY05.
West Point Acceptable Performance	100% by the end of FY05.
Measure of Performance	Charter approved, incorporated in 2010 AT plan; ATEC meets semi-annually, DPTMS maintains minutes of sessions.
Discussion	Reference: , Critical Task 1; DOD I 2000.16 Stnd 12
Budget/Resources	There is no additional cost to implement this goal; the strategy costs are calculated in the salaries of the member's assigned. The resource impact however is removing some members from their primary responsibilities to perform their ATWG functions.

c. Performance Objective 2C: Random Antiterrorism Measure (RAMs).

Performance Objective	- Ensure West Point activities develop and implement RAM as an integral component of the overall AT program guided by the principles outlined in reference (b) DoD O-2000.12H - Ensure West Point activities employ RAM, in conjunction with site-specific FPCON measures, in a manner that portrays a robust security posture from which terrorists cannot easily discern security force patterns or routines. - Ensure Garrison includes tenant commands in RAM planning and execution.
Applies to	West Point activities
Army Baseline	60-70%
ARNORTH acceptable performance	95-100% by end of FY10.
West Point Acceptable Performance	100% by the end of FY11.
Measure of Performance	Activities conducting RAM in conduct of daily duties and cadet training.
Discussion	Reference: AR 525-13, Critical Task 5; DOD I 2000.16 Stnd 14. RAM, at a minimum shall consist of the random implementation of higher FPCON measures in consideration of the local terrorist capabilities.

Budget/Resources	Provide necessary (RAMP) Random Antiterrorism Measures for West Point. Funding is required for training in the use of explosive detection equipment and RAMP Kits for tenant organizations. Signage 1k, Channelize Cones $45 x 50 = 2250, Barrier Tape $90, shipping $210.00 total $2550 Annual training for use of Explosive Detection Equipment $2,450.00 total = $5000.00 with 2.3% inflation FY11- $5K FY12 - $5.2K FY13 - $5.4K FY14 - $5.6K

d. Performance Objective 2D: Comprehensive AT Plans.

Performance Objective	- Ensure West Point develops comprehensive AT Plan that covers at a minimum: - Threat Assessment, Criticality Assessment, Vulnerability Assessment, Risk Assessment, Risk mitigation measures (including RAM), Physical Security measures, Off-installation DoD facilities AT measures (housing and activities), HRP measures, construction and building considerations, Logistics contracting measures, Critical asset security, Incident Response, Consequence Management (including CBRNE and WMD mitigation planning), Site specific FPCON measures
Applies to	West Point
Army Baseline	50-60%.
ARNORTH acceptable performance	100% by the end of FY10.
West Point Acceptable Performance	By end of 3QTR 09, AT plan approved, and reviewed. Plan exercised by end of FY10.
Measure of Performance	By end of 3QTR 09, AT plan approved, and reviewed. Plan exercised by end of FY09.
Discussion	Reference: AR 525-13, Critical Task 7; DOD I 2000.16 Stnd 7. Many Garrisons have AT plans, but they are not comprehensive or are fragmented.
Budget/Resources	There is no additional cost to implement this goal; it is calculated in the ATO salary

e. Performance Objective 2E: Pertains only to RCC's. By the end of 2010 trends will reflect that RCC and US Defense Representatives and Department of State Chiefs of Mission have completed 100% of the required Memorandums of Understanding to clarify AT responsibility for geographic combatant command assigned and non-assigned DoD Elements and Personnel.

f. Performance Objective 2F: West Point FPCON action sets.

Performance Objective	- Ensure West Point has established site-specific actions for each FPCON level.
Applies to	West Point
Army Baseline	60-70%.
ARNORTH acceptable performance	90% by end of 2d QTR FY11.
West Point Acceptable Performance	100% by end of FY11.
Measure of Performance	Site specific actions developed and approved for each FPCON measure; actions incorporated into AT plan; West Point activities briefed and trained on actions.
Discussion	Reference: AR 525-13, Critical Task 5, DOD I 2000.16 Stnd 14
Budget/Resources	There is no additional cost to implement this goal; it is calculated in the ATO salary

g. Performance Objective 2G: Installation Preparedness Measures.

Performance Objective	- Establish Installation Preparedness Measures that address mass warning systems, CBRNE detectors and monitors, collective protection and individual protective equipment.
Applies to	West Point Garrison
Army Baseline	20-30%.
ARNORTH acceptable performance	90% by end of 2d QTR FY10.
West Point Acceptable Performance	Mass warning system purchased FY09 and in place by end of 2d qtr FY11; DES HAZMAT team equipped and trained by end of FY09, CBRNE detectors and monitors purchased and installed by the end of FY10.
Measure of Performance	Mass warning system purchased and in place by end of FY09; DES HAZMAT team equipped and trained by end of FY09, CBRNE detectors and monitors purchased, personnel trained, and installed by the end of FY11.

Discussion	Reference: AR 525-13, Critical Task 7; DOD I 2000.16 Stnd 21
Budget/Resources	One year warranty for Dialogic telephone Mass Notification System. Baseline cost of $30000.00 used, and 10% inflation used for out years. One year warranty for Giant Voice Mass Notification System. Baseline cost of $14000.00 used, and 10% inflation used for out years. FY11- $41.2K FY12 - $49.4K FY13 - $54.2K FY14 - $59.5K

h. Performance Objective 2H: Mutual Aid Agreements (MAAs), Memorandum of Agreement (MOA), and Memorandum of Understanding (MOU's).

Performance Objective	- Ensure Garrison and tenant units develop MAAs, MOAs or MOUs with off-installation/facility civilian authorities to support AT Plan.
Applies to	DES, KACH, DPTMS
Army Baseline	30-40%.
ARNORTH acceptable performance	95-100% by end of FY 2010.
West Point Acceptable Performance	MOAs updated by end of FY11.
Measure of Performance	DES - MOAs updated with local, county and state law enforcement/first responder agencies; KACH – MOAs with local hospitals; DPTMS–MOA with Stewart Airport security regarding 2nd Aviation's security.
Discussion	Reference: AR 525-13, Critical Task 6; DOD I 2000.16 Stnd 21
Budget/Resources	There is no initial cost implement this goal, the strategy costs are calculated in the salaries of the member's assigned (ATO, DES, SJA, etc…). During certain times when the MOA/MOU has to be initiated there may be costs associated with the level of support received from the various agencies. Those costs are captured in the installations emergency funds as required.

i. Performance Objective 2I: AT Building Construction Standards.

Performance Objective	- Ensure West Point implements AT construction and mass notification systems standards to new constructions and major renovation, repair, and restoration projects.
Applies to	DPTMS, DPW, Corps of Engineers
Army Baseline	70-80%.
ARNORTH acceptable performance	95-100% by end of FY10.
Acceptable	100% by the end of FY11.

Performance	
Measure of Performance	Percentage of construction projects that have adhered to DoD AT Building construction standards. (UFC 4-010-01).
Discussion	Reference: AR 525-13, Critical Task 7 and paragraphs 2-7 and 2-15; DOD I 2000.16 Stnd 17 and 28.
Budget/Resources	There is no additional cost to implement this goal, the strategy is calculated in the ATO salary; however, after the review there are additional costs that will be absorbed in the construction costs. Those costs are funded through military construction projects through congress.

4. Strategic Goal #3: Conduct effective AT training and execute realistic AT exercises. This goal contains five West Point supporting performance objectives listed below:

a. Performance Objective 3A: IAW Army and USNORTHCOM Strategic Plans incorporate AT and CBRNE exercises simultaneously into all operations, training, including exercises with local civilian agencies. By the end of 2011 will reflect that Commanders have incorporated AT training into all (100%) operations and exercises.

b. Performance Objective 3B: AT Awareness (Level I).

Performance Objective	- West Point activities shall establish and sustain policies and procedures to ensure that Soldiers, civilian employees, contractors, and DoD Family members ascertain the appropriate AT awareness training and document annual completion.
Applies to	West Point activities
Army Baseline	50-60% by end of FY09
ARNORTH acceptable performance	90% by end of FY10
West Point Acceptable Performance	100% By end of FY11.
Measure of Performance	Activities and tenant units ensure employees, contractors, soldiers and cadets receive AT level I training annually, receive AT level I retraining within 6 months of traveling OCONUS; employees, cadets, soldiers and family members over the age of 14 receive a AOR specific briefing prior to traveling OCONUS. DPTMS tracks status of AT level I training; tracks travel information for those traveling OCONUS.
Discussion	Reference: AR 525-13, Critical Task 4; DOD I 2000.16 Stnd 25
Budget/Resources	There is no additional cost to implement this goal; the strategy is calculated in the ATO salary.

c. Performance Objective 3C: Antiterrorism Officer Training (Level II).

Performance Objective	- Ensure West Point designates the ATO in writing, and ensures that the ATO attends a Level II Certified course of instruction.
Applies to	DPTMS and West Point activities
Army Baseline	70-80%.
ARNORTH acceptable performance	95-100% by end of FY07.
West Point Acceptable Performance	100% by the end of FY05.
Measure of Performance	Level II certified ATO on orders under direction of DPTMS.
Discussion	Reference: AR 525-13, Critical Task 1; DOD I 2000.16 Stnd 26
Budget/Resources	Provides Temporary Duty (TDY) for one full time ATO; travel funds to attend Level II AT training course to certify ATO to serve as the commanders AT advisor and AT instruction. Max per diem rate for Fort Leonard Wood, MO ($109) multiplied by 15 days = Per Diem x days x personnel x trips = $1635.00, Per Diem 7 days @ $109 a day x 1 personnel = $1635.00, Travel cost for 1 air line tickets at $800.00 each = $800.00, Rental car @ $150 per week X 1 trips = $150 Total = $ 2585.00. This is for Level II Certification

d. Performance Objective 3D: High Risk Personnel (HRP) Training. Does not pertain to West Point; pertains only to MACOMs and RCC's. By the end of 2007, trends will reflect that MACOMs and Combatant Commanders have incorporated AT training into all (100%) operations and exercises.

e. Performance Objective 3E: Commanders Training (Level III).

Performance Objective	- Ensure Garrison Commander receives Level III Commanders training.
Applies to	USAG Commander
Army Baseline	60-70%.
ARNORTH acceptable performance	95-100 by end of FY09
West Point Acceptable	100% by the end of FY10,

Performance	
Measure of Performance	Garrison Commander completes the Army Level III Commanders training.
Discussion	Reference: AR 525-13, Critical Task 4; DOD I 2000.16 Stnd 29
Budget/Resources	There is no additional cost to West Point to implement this goal, the costs associated with this strategy is absorbed by higher headquarters.

f. Performance Objective 3F: Comprehensive Training Exercises.

Performance Objective	- Ensure West Point develops and executes comprehensive training exercises that test: CBRNE, WMD, and FPCON capabilities measures.
Applies to	West Point activities
Army Baseline	40-50%. by end of FY09
ARNORTH acceptable performance	95-100% by end of FY10
West Point Acceptable Performance	Training exercise that assesses capability of installation activities to respond to chemical and explosive threat by end of FY10; training exercise assessing capability of installation activities to respond to biological and radiological threat by end of FY11;
Measure of Performance	Number of installation activities participating and responsive to specific CBRNE threat
Discussion	Reference: AR 525-13, Critical Task 8; DOD I 2000.16 Stnd 23
Budget/Resources	To enhance exercise program support the WMD and MASCAL AT plans and procedures and to participate and conduct exercise with our local committees along with Orange County and NY State Office of Emergency Management. Funds will allow for support to the installations Exercise program to bring evaluators to West Point to allow the Senior Commander's staff to train, participate, and be tested rather than observe and critique. Cost driver also supports the purchase of vehicles/airplane to add realism. Additionally funds will also to support joint exercises with local government emergency agencies and exercise designer and evaluators. FY11- $10.3K FY12 - $10.5K FY13 - $10.8K FY14 - $11.1K

g. Performance Objective 3G: Primary Duty ATOs.

Performance Objective	- Ensure antiterrorism is the primary duty of installation ATO.
Applies to	DPTMS, West Point activities
Army Baseline	95-100%.
ARNORTH	95-100% by end of FY09.

acceptable performance	
West Point Acceptable Performance	100% by the end of FY05.
Measure of Performance	Trained individual with antiterrorism as assigned primary duty
Discussion	Reference: AR 525-13, paragraph 2-9; DOD I 2000.16 Stnd 5.
Budget/Resources	Salary - AT Program Management (Personnel, ATO) 1 FTE, existing ATO, Funding is required for one AT Program Manager (GS-12) required to run and support AT programs. These values reflect; annual West Point salary plus locality pay for New York, The ATO civilian pay is based on a base line salary of 83.2K with a 2.3% inflation rate. Using the payroll estimator the cost driver was calculated using the Annual Salary for Locality @ Step 5 + Employee Benefits @ 30% + Awards @ 1.5% with a 2.3% inflation rate. FY11- $115.5K FY12 - $118K FY13 - $121K FY14 - $123.5K

5. Strategic Goal #4: Optimize the planning, programming, and execution of resources, including Research, Development, Test, and Evaluation (RDT&E) in support of AT programs.

This goal contains six West Point supporting performance objectives listed below:

a. Performance Objective 4A: AT Program Analysis.

Performance Objective	- Implement and enhance policy and procedures to meet ARNORTH AT requirement documentation and prioritization methodology
Applies to	West Point activities
Army Baseline	70-80%.
ARNORTH acceptable performance	100% by end of FY06.
West Point Acceptable Performance	100% by the end of FY06.
Measure of Performance	Activities provide input to Garrison; Garrison develops Schedule 75 funding requirements and prioritization; ATWG reviews; ATEC approves.
Discussion	Reference: DoD I 2000.16, Stnd 26.
Budget/Resources	There is no additional cost to implement this goal; the strategy is calculated in the ATO salary.

b. Performance Objective 4B: Combating Terrorism Readiness Initiative Fund (CbT RIF).

Performance Objective	- Ensure West Point complies with CbT RIF requirements and POM submissions for emergent and emerging AT requirements.
Applies to	DPTMS, G-3
Army Baseline	90-100%.
ARNORTH acceptable performance	100% by end of FY10
West Point Acceptable Performance	100% by the end of 2011.
Measure of Performance	CbT RIF submissions submitted through CVAMP; FP/AT requirements prioritized and properly documented on Schedule 75
Discussion	Reference: DoDO 2000-P, strategic goal 4
Budget/Resources	There is no additional cost to implement this goal; the strategy is calculated in the ATO salary.

c. Performance Objective 4C: Budget Execution for AT-Related Expenditures

Performance Objective	- AT budget execution will reflect execution for intended purpose of AT-related expenditure
Applies to	USAG
Army Baseline	75%.
ARNORTH acceptable performance	85% by the end of FY09. 95% by the end of FY10, 100% by the end of FY11
West Point Acceptable Performance	Providing quarterly execution reports to NERO by the end of 2010
Measure of Performance	Quarterly execution reports from West Point garrison to IMCOM-NE
Discussion	Reference: DoD O-2000-12-P, Strategic Goal 4
Budget/Resources	There is no additional cost to implement this goal; the strategy is calculated in the ATO salary.

d. Performance Objective 4D: Core Vulnerability Assessment Management Program (CVAMP).

Performance Objective	- Ensure West Point utilizes and implements fully the Core Vulnerability Assessment Management Program (CVAMP).
Applies to	West Point
Army Baseline	40-50%.
ARNORTH	95-100% by end of FY10.

acceptable performance	
West Point Acceptable Performance	100% by the end of FY10.
Measure of Performance	AT vulnerabilities and AT protective measure shortfalls fully documented through CVAMP.
Discussion	Reference: AR 525-13, paragraph 2-9; DOD I 2000.16 Stnd 6 and 30
Budget/Resources	There is no additional cost to implement this goal; the strategy is calculated in the ATO salary.

e. Performance Objective 4E: Technologies, Equipment, and Process.

Performance Objective	- Research and field innovative technologies, equipment, and processes that enhance AT readiness
Applies to	West Point
Army Baseline	60-70%. (Trends based on action required)
ARNORTH Acceptable Performance	TBD-By ARNORTH
Measure of Performance	Subjective analysis of new or improved technologies, equipment, and process identified to improve AT shortfalls.
Discussion	Reference: TBD
Budget/Resources	Initially there is no additional cost to implement this goal, however, AT resource requirements using the Planning, Programming, Budgeting, and Execution process needs to be completed prior to providing an actual dollar sign to a goal. Also the process must use the Department of the Army approved methodology for documenting and prioritizing AT resource requirements. This process takes an average of two years. Budget request for FY13 – FY15 FY11- $0K FY12 - $0K FY13 - $200K FY14 - $215K FY15 - $230K

f. Performance Objective 4F: Mitigated Vulnerabilities or Assume Risk.

Performance Objective	- Ensure West Point activities have mitigated vulnerabilities by funding decisions, improved security TTPs, risk reassessed at a lower acceptable level, or risk assessed and assumed in writing
Applies to	West Point activities
Army Baseline	40-50%.
ARNORTH acceptable	71-74% by end FY 2009

performance	
West Point Acceptable Performance	75-85% by end of FY10. 100% by the end of FY11
Measure of Performance	Number high-risk vulnerabilities for critical assets/special events mitigated or vulnerability assumed in writing.
Discussion	Reference: 525-13, Critical Task 3; DOD I 2000.16 Stnd 3
Budget/Resources	There is no additional cost to implement this goal; the strategy is calculated in the ATO salary.

6. Strategic Goal #5: Execute holistic, comprehensive reviews of AT programs to ensure compliance with ARNORTH AT Program standards. This goal contains two West Point supporting performance objectives listed below:

a. Performance Objective 5A: Pre-Deployment AT program review. Does not pertain to West Point; pertains only to MACOMs and RCC's. By the end of 2006, 95-100% of all Army commands with deploying units shall have conducted pre-deployment AT program review.

b. Performance Objective 5B: Does not pertain to West Point; pertains only to RCC's. By the end of 2007, all Combatant Commands, Defense Agencies, and DoD Field Agencies shall have undergone at least one Joint Staff-led HHA within three years to assess command-wide compliance with references (c) and (d).

c. Performance Objective 5C: Annual Review of AT Program.

Performance Objective	- Ensure West Point conducts an annual review of the AT program.
Applies to	West Point activities, DPTMS
Army Baseline	60-70%.
ARNORTH acceptable performance	95-100% by end of FY09.
Acceptable Performance	100% by the end of FY06.
Measure of Performance	ATWG conducts annual review of AT program. Results briefed and approved by ATEC
Discussion	Reference: AR 525-13, paragraph 2-9; Critical Task 3, DOD I 2000.16 Stnd 31
Budget/Resources	There is no additional cost to implement this goal; the strategy is calculated in the ATO salary.

d. Performance Objective 5D: Joint Service Integrated Vulnerability Assessment (JSIVA)/

Higher Headquarters Assessment (HHA).

Performance Objective	- Ensure that West Point undergoes a JSIVA/HHA within past three years.
Applies to	West Point
Army Baseline	90-100%.
ARNORTH acceptable performance	90-94% by end o FY08.
West Point Acceptable Performance	100% by the end of FY05.
Measure of Performance	Ensure that either JSIVA or IMCOM HHA is scheduled within a three years of previous assessment.
Discussion	Reference: 525-13, Critical Task 3; DOD I 2000.16 Stnd 31
Budget/Resources	There is no additional cost to West Point to implement this goal, the costs associated with this strategy is absorbed by higher headquarters.

7. STRATEGIC GOAL #6: Develop a reporting and evaluation system that provides effective and timely data sufficient to apply resources to adjust the program for a changing environment. This goal contains no West Point supporting performance objectives listed below:

a. Performance Objective 6A: Army AT policy. Pertains to ARNORTH revising the Army AT policy in AR 525-13 by 2007.

b. Performance Objective 6B: Army AT reporting system. Pertains to ARNORTH developing a reporting system to evaluate the Army AT program by 2010.

c. Performance Objective 6C: Assessments of major Army subordinate headquarters. Pertains to ARNORTH revising the Force Protection Assessment Team by 2010.

d. Performance Objective 6D: Resources guidance and priorities. Pertains to ARNORTH providing guidance and assistance to subordinate headquarters in planning for AT improvements.

8. STRATEGIC GOAL #7: Embed AT concepts throughout the Army by developing, implementing, and sustaining AT training and doctrine for Army military and civilians. This goal contains one West Point supporting performance objective as indicated below:

a. Performance Objective 7A: Army AT doctrine. Does not pertain to West Point. By 2009 there will be a draft Army AT field manual draft and final publication in 2011.

b. Performance Objective 7B: Army AT training in professional military education (PME) for military and civilian

Performance Objective	Integration of AT into all officer, NCO PME and civilian training to ensure long term development of knowledge and skills.
Applies to	Dean, Commandant
Army Baseline	20-30% of Officer, NCO and civilian courses integrate AT into their curricula
ARNORTH Acceptable Performance	30-40% by 2008, 50-60% by 2009, 80-90% by 2010, 100% by 2011
West Point acceptable performance	By end of FY10
Measure of Performance	Commandant: Incorporate AT into realistic cadet field training exercises. Use the experiences and lessons learned by staff and faculty in combat operations to enhance cadet experience with AT as it applies to tactics, techniques and procedures; provide academic courses in low intensity conflict, insurgency and counter-insurgency operations; Dean: establish a Center for Combating Terrorism that supports the war against terrorism through education, research and policy analysis; host conferences to promote the study of insurgency and terrorism. Leverage the operational and academic expertise of the staff and faculty to provide the cadets and officers with the opportunity to study terrorism.
Discussion	Reference: AR 525-13, paragraph 2-14. a. (2). Not fully implemented as of this Plan. Long term improvement and implementation of effective AT program depends upon a solid training base for all grades, skills, and functional areas.
Budget/Resources	There is no additional cost to West Point to implement this goal, the costs associated with this strategy is absorbed by higher headquarters.

c. Performance Objective 7C: Improvement of Army Level III Training for prospective commanders; does not pertain to West Point. By 2009 there will be a directive issued with full implementation by 2010 in all pre-command courses.

d. Performance Objective 7D: Train senior executives and key leaders. This does not pertain to West Point. Instruction provided for all key leaders (other than battalion/brigade

commanders) who are responsible for programs or involved in AT policy, planning, and execution.

References

(a) DoD O- 2000.12-P, “DoD Antiterrorism Strategic Plan,” June 15, 2004

(b) DoD O-2000.12-H, "DoD Antiterrorism Handbook," February 9, 2004

(c) DoD Instruction 2000.16, “DoD Antiterrorism Standards,” October 2006

(d) DoD Directive 2000.12, “DoD Antiterrorism Program,” August 18, 2003

(e) DoD Instruction 2000.18, “DoD Installation Chemical, Biological, Radiological, 6. Nuclear, and High-Yield Explosive Emergency Response Guidelines,” December 4, 2002

(f) United Facilities Critical (UFC) 4-010-01, “DoD Minimum Antiterrorism Standards for Buildings,” January 2007

(g) United Facilities Critical (UFC) 4-010-02, “DoD Minimum Standoff Distances for Buildings,” January 2007

(h) United Facilities Critical (UFC) 4-021-01, “Design and O&M: Mass Notification Systems,” December 18, 2002

(i) Deputy Secretary of Defense Memorandum, “Collection, Reporting, and Analysis of Terrorist Threats to DoD Within the United States.” (GUARDIAN), 13 SEP 07

(j) Antiterrorism Strategic Plan for the United States Army, “Forging the Shield”, August 2005

(k) Army Regulation 525-13, “Antiterrorism,” September 2008

(l). Army Regulation 190-58, “Personal Security,” 22 March 1989

Bryson John M., Strategic Planning for Public and Non Profit Organizations, Jossey-Bass, San Francisco, CA, 3rd Edition

Chapter 4

U.S. Constitution and Ethical Issues: Homeland Security Management

"I would rather be exposed to the inconveniences of too much liberty than to those attending too small a degree of it."

Thomas Jefferson

"The Constitution is the bedrock of all our freedoms; guard and cherish it; keep honor and order in your own house; and the republic will endure."

President Gerald R. Ford

Homeland Security: A Threat to Civil Liberties or an Instrument of National Security

Terrorists have wreaked havoc on civilizations throughout time, but for many Americans the tragedy that happened on September 11, 2001 has been on all of our minds. It was an act of hate that we are not going to forget anytime soon. But through all the tragedy, we still stand strong as a nation. We are here to fight for what we believe in. The acts on September 11th may have destroyed our buildings, but it did not destroy our spirit. History has shown that American people, organizations, and facilities make lucrative targets for a terrorist or criminal attack. The future predicts little change. Attacks on personnel and facilities by individuals and organizations operating outside the formal command and control structure of national governments have claimed many lives; the cost to the U.S. Government and private industry is measured in billions of dollars.

A citizen of the United States has a reasonable belief that security will be provided for her or him by law enforcement officials. Some of the laws enacted by the government are because of a certain threat or because there is reasonable belief that law enforcement officials are

in need of certain tools to maintain a particular level of security. As new laws will be voted in to thwart activities in the ever-changing environment that the war on terrorism brings, a potential exists for some to feel that civil liberties will be infringed or taken away. Others, after educating themselves about the new laws, will understand and support the government for the good of the country. The people who occupy this great country are from the four corners of the earth and all points in between. At what point should a government by the people decide that civil liberties are more important than the security of its people?

The purpose of this Masters Project paper is to provide an overview of the constitutional amendments that apply to securing our nation. There are a total of twenty-seven amendments to the Constitution. In my opinion not all of the amendments are pertinent to the defense of the homeland. Amendments I through X are the Bill of rights. This paper will address the amendments that I believe are relevant to the defense of our nation and could possibly be endangering our constitutional rights. Additionally this paper will discuss the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism, better known as the PATRIOT Act.

The U.S. Constitution demonstrates that the founders were extremely concerned about the government's ability to abuse its power and violate the liberties of the people contained in the Bill of Rights, including the rights of an accused in criminal procedures. Under what specific circumstances should terrorist suspects have the same constitutional rights that criminal suspects have in the criminal justice system?

The Bill of Rights

The Bill of Rights has become an extremely controversial topic since 9/11. The government’s techniques of investigation, detainments, and prosecution in the name of national

security have been challenged and will continue to be, as America continues its attempt to find a balance between liberty and security. Today America is faced with a challenging question: what is to be done about terrorism? There are no easy answers to this question. Specifically should terrorist suspects have the same constitutional rights that criminal suspects have in our criminal justice system? First and foremost, let us dispense with the notion that these terrorists deserve the rights that are protected by the Constitution. As stated in the Preamble to the Constitution, said document was drawn up for the purpose of protecting the liberties of the citizens of the United States. Nowhere do you see a clause protecting those who wish to do harm to our government or private citizens:

> We the people of the United States, in order to form a more perfect union, establish justice, insure domestic tranquility, provide for the common defense, promote the general welfare, and secure the blessings of liberty to ourselves and our posterity, do ordain and establish this Constitution for the United States of America.
>
> (Preamble to the Constitution)

None of the subsequent articles or amendments makes any provisions for enemies of the United States except possibly for the Fifth Amendment which states the following: "No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a grand jury, except in cases arising in the land or naval forces, or in the militia, when in actual service in time of war or public danger…" (Constitution)

This paper will discuss each of the constitutional amendments that I believe are applicable to defending our great nation. After 9/11 there was increased concern about the First Amendment and burning the flag or protesting. Amendment I concerns the freedom of religion, speech, the press, and right of petition. I believe that in these times, the freedom of

speech needs to be viewed as an issue for defending our homeland. On November 5, 2009 U.S. Army Major Nidal Malik Hasan killed 13 people and wounded 30 others at the Army base in Fort Hood, Texas. Soon after the attack, on his website Anwar al-Awlaki praised Hasan for the shooting, declared him a hero, and encouraged other Muslims serving in the military to "follow in the footsteps of men like Nidal" as well as "fighting against the U.S. army is an Islamic duty". This is just one example where I don't believe the freedom of speech should be allowed. The U.S. government is currently working on a bill entitled the Cyber Security Act of 2009 which would give the President unprecedented powers over the internet, including the ability to "shut down" portions of it when a cyber security emergency is declared." The issue at hand is how we determine a cyber emergency and who should make that determination. The president is elected by the people, for the people. The president then makes choices to fill key positions within the federal government. In this particular case the Director of National Security with various other agencies should determine what establishes a cyber emergency and make a strong recommendation to the president to shut down the internet. Some would say this is totally against our constitutional rights; I would have to agree to an extent but the government does need a tool to curb the actions of individuals such as Julian Paul Assange of WikiLeaks. Assange is nothing more than a web-type reporter looking for fame. The individuals who provide the information are criminals acting against the United States (McDougall, P). Another issue is that the U.S. doesn't know the extent of the damage that has been caused by WikiLeaks, so the government should use extreme caution with this extraordinary power and not have an automatic reaction every time something is posted to the internet. The bottom line in regards to the WikiLeaks issue is that the individuals who released the documents should be prosecuted to the fullest extent of the law. The specialist, if convicted will be crucified; the military justice system

is much tougher than the civilian courts. Unfortunately the civilian who leaked the documents from the State Department will only be prosecuted in federal court.

The one area that I feel the government overstepped its boundaries was during the BP Oil crisis in the Gulf region. They pledged to allow footage of the entire incident but would not allow cameras or reporters to film the actual devastation **(**Nimmo, K). This is one instance where at the public has the right to know what's going on. I am a true believer in the Constitution and upholding it, but there are some things that the citizens do not need to know about security. For example, in a *Washington Post* news story titled "Electric Utilities May Be Vulnerable to Cyber Attack" by Ellen Nakashima and R. Jeffrey Smith in April 2009 discusses the vulnerabilities of the United States. Numerous television news shows also feel obligated to announce to the world that we have vulnerabilities and often explain in detail how to exploit them. In these cases the First Amendment should not be used as an excuse. This type of reporting should not be allowed until such time as the issues were reported and addressed; if not addressed, then they can be reported. The media is essential but should not be allowed to report or possibly be informed of an investigation until it is completed or an arrest has been made. Originally I would have said "until tried and convicted or acquitted," since reporting should be done after the arrest and investigation. This does two things: first, it doesn't interfere with or follow the investigation and second, it provides some comfort to the citizens knowing we have the capability to capture the suspects.

The Fourth and Fifth Amendments are designed to protect citizens from unlawful practices from both law enforcement agencies and government harassment. Additionally, there have been recommendations for changes to the Constitution because the main concerns will always be generated over individual freedoms versus individual security. But at the same time

we as Americans have and enjoy our freedoms and even if rules or laws are changed, how much will it truly affect our freedoms. When the rest of the world sees free individuals, but mostly Americans, they already have pre-conceived images as the ones living up to the old Cold War stereotypes and so-called propaganda from the communist countries. Freedom has this affect of making you proud. The American display of freedom can sometimes present an atmosphere that leaves something to be desired. The perception of others is that we are arrogant and are always right; we want to impose our will and opinions on others. When you have freedom, you feel that this is your right and you can act this way, and if members of society do not like it, they can leave because I am free to do as I please. However, sometimes these freedoms we hold so close are misinterpreted and twisted by certain individuals and end up working against us. These refer to the threatening individuals like Ted Kazinsky, Tim McVeigh, and Lee Malvo who are examples of irresponsible, insensitive behavior.

The Fourth Amendment states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized" (Cornell).

The United States Government is working to prevent terrorist attacks from ever again recurring on American soil. Airline security for the most part has tightened up tremendously. There are new screening technologies that are making their way to airports, and security screeners question all suspicious people. Most recently the use of full body scanners has been an issue of contention. The executive director of the Association for Airline Passenger Rights (AAPR) states "the enhanced full-body scanners and aggressive pat-downs, among other things, violate privacy rights protected by the U.S. Constitution's Fourth Amendment." Macsata

further states the various civil liberties groups also feel this way. He also complains that the TSA chose to introduce the scanners during the busy holiday season. What Macsata fails to mention is that past events have happened during the holiday season, for example the underwear bomber, Umar Farouk Abdul, and the attempt at the Portland holiday tree lighting by Mohamed Osman Mohamud to name a couple. Additionally Mascara doesn't mention that flying on commercial aircrafts isn't necessarily a right afforded by the Constitution. It's a privilege and safety and security does matter for all those that are travelling on those aircraft.

The Fifth Amendment provides for due process under the law. It states that "No person shall be held to answer for any capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation" (Cornell).

On September 9, 2005, the Forth Circuit Court of Appeals upheld the federal government's authority to detain an American citizen arrested within the United States indefinitely without charging him with a crime. All the president has to do is call a citizen an "enemy combatant" and the person's due process rights disappear. Judge J. Michael Luttig wrote the Court's unanimous decision which contends that a post-9/11 Congressional resolution gave the president "the power to detain identified and committed enemies such as Padilla, who associated with al Qaeda and the Taliban regime, who took up arms against this nation in its war against these enemies, and who entered the United States for the avowed purpose of further

prosecuting that war by attacking American citizens and targets on our own soil" (Gregory, A). Another example is the case of Hady Hassan Omar who was held without trial and placed in solitary confinement for 73 days. For a long period after his arrest, he was not allowed access to an attorney. One of prison guards told him, "The Attorney General just signed a new law today. We can keep you here as long as we like." He was subjected to repeated interrogations. He threatened hunger strikes but was told by prison officials that they would just strap him to a gurney and force-feed him through a tube up his nose. After 73 days, he threatened suicide and finally officials decided that he was innocent and released him. If an American citizen, whether born or naturalized, is suspected of terrorism, there should be a maximum amount of time that such a person can be held without having the representation of a lawyer; 30 days is long enough for the federal government to make a case, after such time a lawyer must be allowed.

One of the reasons we are fighting the terrorists is to protect our way of life. This way of life includes our protection from our government and our rights to fair trials given to us by the Constitution. In a way it is hypocritical of us to fight, so we maintain our freedoms while depriving other of those same freedoms. Our country has not given many of our captured suspected terrorists a status to define how to deal with them. By this I mean they are not prisoners of war because the Congressional Resolution after 9/11 was not a declaration of war. Therefore they are not given protection by the normal conventions and laws of war. The laws governing due process do not apply to enemy combatants so they are not afforded Constitutional protections either (Gregory, A).

The Sixth Amendment concerns civil rights in trials for crimes enumerated. "In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury… and to be informed of the nature and cause of the accusation; to be confronted

with the witnesses against him; to have compulsory process for obtaining witnesses in his favor and to have the assistance of counsel for his defense" (Cornell).

The reasons for holding these persons are the possibility they may have access to information to prevent attacks or may have been involved in an attack themselves. It is vital to our national security to obtain this information. The big issue in my opinion is how far we are willing to go to get it. The balance between liberty and security has to be maintained somehow. Our court system is not made to handle the issue of foreign terrorists and enemy combatants. A system independent of our court system, perhaps an international court, should be established to handle this issue. For example, if a case involves people from different states, it is normally handled at a federal level. To apply this concept to this situation, an international court could handle the case between people from different nations.

Military tribunals or commissions have a unique process that most American citizens do not understand. They aren't military courts-martial nor are they civil law. Therein lies the problem; they have the ability to process detainees within unspecified or unclear parameters. The terrorists should be tried for their crimes but they do not meet the criteria set forth in the Bill of Rights and U.S. Constitution. Their status is unknown and indefinable to date. It was thought the PATRIOT Act was going to create a path to conviction and punishment of the terrorists and their co-conspirators, but as we have witnessed, several appeals have made their way through our court system. In addition, because of those appeals, President Bush, via the PATRIOT Act, lost several of his efforts to hold those responsible for their actions against Americans and our allies. An Oregon judge said this act gave too much power to the government when it came to "snooping on suspected criminals in the United States," a violation of constitutional search-and-seizure rules. That decision led to the following: "A federal appeals court ruled that some

portions of the U.S. PATRIOT Act that govern dealings with foreign terrorist organizations are unconstitutional because the language is too vague to be understood by a person of ordinary intelligence" (Democratic Underground). The PATRIOT Act measures have good intentions and can sometimes get distorted. Is there a danger that this act may be used against law abiding citizens as with any law or act? The answer is yes, but as anything that is created by people, it will not be perfect.

As stated by Bobby Chesney and Jack Goldsmith, Wake Forest and Harvard, respectively, "Neither the criminal nor the military model of detention of terrorists can easily meet the central legal challenge of modern terrorism." Criticism of the terrorists' due process is heard from both sides of the aisle and each has its merits whether we agree with them or not. Civil courts maintain the civil liberty protection of all within the United States and the military court-martial system serves the uniformed personnel. So how does law define the terrorists? Most are not citizens, they are not combatants in respect to our military definition, and the term "prisoner of war" does not apply to them either. In effect, terminology has foiled our attempts to try to convict them.

According to Matthew Purdy's article in the *New York Post* dated November 25, 2001, the inception of the military tribunals would "promise to be swift and largely secret, the release of information likely to be limited to the barest facts, and the transcripts of the proceedings could be classified and kept from public view for years." The tribunals would give authorities the ability to detain and prosecute people suspected of terrorism. It also needs to be noted when President Bush announced his new military law, he said he had "strong public support" of the measure; his support has since eroded into a massive legal cluster of appeals. The erosion evolved because of the American dislike of what is seen as the basic human rights of law. Those

include the right to a jury trial and the protection of the attorney-client relationship and the lengthy detentions the legal hawks have called illegal. The measure of secrecy of the military tribunals has also added to increased questioning.

The Supreme Court is weighing the pluses and minuses of the tribunals. Do the terrorists have the right to a speedy trial without the lengthy detention as required by law or are the rules changed to suit the commissions? Tribunals are not required to adhere to the basic law of the US. Their evidentiary procedures are more lenient since hearsay and coerced testimony are admissible, and the defendant and his lawyers are not privy to the evidence. In addition, they are secretive, the jury consists of a majority of military officers, the convictions and sentences are meted with a "majority-rule," and the judgment cannot be appealed except by the President, who secured the tribunal in the first place. Those who reject the tribunal system insist the civil courts would provide a better trial venue for several reasons, one of which is the swiftness of a trial. The languishing of terrorists in a military system would be greatly diminished freeing them up for other duties; it is a fact that the civil courts have a better record of convictions than the tribunals.

Perhaps one of the most startling deterioration of human rights is the right of the attorney general to decide who is deemed a terrorist and should be detained. Simply stating he has "reasonable grounds to believe" a person is or may be part of a terrorist group allows the U.S. to jail a person. This can and has raised a red flag as seen in the case of Murat Kurnaz who was held as an enemy combatant for five years. Both the U.S. and German investigators in the case found no evidence that he was involved in terrorist activities other than the claim by three military officers that they has supposedly confidential information claiming otherwise. After his files were leaked to the public, it was found there was no substantiating information and he was

released. Although this is one case, there since have been others released under the same precedent. Does our government have the duty to ensure they are detaining the right people and to oversee the "experts" who make the "enemy noncombatant" determination? The Global War on Terrorism opened numerous doors and unexplored areas that will not be answered for years. In 1787 the Constitution gave the president broad powers in times of war as commander-in-chief of the armed forces (Article II, Section 2). It also gave Congress the power to define and punish offenses against the law of nations (Article I, Section 8, Clause 10). "The Congress shall have Power to…provide for the common Defense and general Welfare of the United States…To constitute Tribunals inferior to the Supreme Court." Although there has been no formal declaration of war, this is the closest we have to making a determination on detainees.

The result of the question of military tribunals versus civil liberties is that the United States must make sure the rules of engagement are the same for all concerned. Providing one government agency as the sole decision-maker is unwise. Further, the concept of terrorism must be identify and quantified. There is not one definition for a terrorist. The military, judicial system, the American public and others define it differently according to circumstances. One such definition is: "A terrorist activity has been broadened to include any foreigner who uses 'dangerous devices' or raises money for a terrorist group, whether or not he or she knows the group is engaged in terrorism." If true, then we need to use this to prosecute those under that definition. However, the Attorney General's office has added, for his use, "If he, the attorney general, simply has 'reasonable grounds to believe' that the person may be a threat, that person can be held indefinitely." Given that, the definition of terrorist has changed significantly.

Whichever side one chooses to sit on, the rights of a terrorist is necessary if only to prevent those like Kurnaz from being mistreated and wrongly held. For those who fall into the

category of terrorist, let us prosecute them quickly and with a trial. The American public is not ignorant of what is going on in the world. They will make the correct choice in convicting those accused of the atrocities and it will take less time than the military tribunal. The choice is not an easy one, but it would alleviate the necessity of legal appeals and waiting for the Supreme Court to make a ruling.

Our country has not given many of our captured suspected terrorists a status to define how to deal with them. By this I mean they are not prisoners of war because the Congressional Resolution after 9/11 was not a declaration of war. As such they are not given protection by the normal conventions and laws of war. The laws governing due process do not apply to enemy combatants so they are not afforded constitutional protections either.

At a minimum the terrorist should be afforded status other than "enemy combatant" so that either our due process or international conventions can apply to them. Either makes them a prisoners of war (The War on Terror) or declares them a criminal and charges them with something. To allow the government to take due process from one is the beginning of the proverbial "slippery slope" to taking liberties from all. Our nation affords the same rights to anyone within its borders, even if they are not here legally. If we give constitutional protection to people who are not citizens here, shouldn't we do so across the board? While the patriot in me says just let them rot, I think ultimately this is the most un-American thing we can do.
Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act)

Soon, if not already, history books and teachers will be teaching and enlightening people on the events that took place on that dark and dangerous day in September. But not only will the events of 9/11 be revealed, the acts and laws put into place in response will hopefully be

explained as well. One act in particular should be explained and understood by children and adults nationally, the USA PATRIOT Act. After 9/11 terrorist attacks, a new act was implemented to secure America and deter incidents alike. This act is referred to as the USA PATRIOT Act, but is defined as "The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" (Lithwick, D). Not only is this act allowing the government to tap into personal cell phones and information, it is blindsiding society into handing over their civil liberties with no real knowledge of what this act entails

The PATRIOT Act introduced an excess of legislative changes which significantly increased the surveillance and investigative powers of law enforcement agencies in the United States" (2). This organization goes on to state, "that there is nothing to verify whether these new powers would be controlled; nobody is watching those who are watching us (USA PATRIOT Act)." Of the many discussions that could take place based on this type of thinking, there are three ideas that immediately come to mind. The first is that there is no trust in law enforcement personnel to use these new powers judicially and that there is no system to prosecute those who abuse these powers. The second thought is that we do not have a watchdog watching the watchdog; at what point or layer of watchdogs do we feel our civil liberties will be protected? Finally, who is to decide what level or layer of people watching people will suffice and will they be knowledgeable in counter/anti-terrorism?

Currently, there are several cases before the courts throughout the nation whereby law enforcement officials who have misused their new authority are being tried. It is tragic when an official exercises poor judgment, but justice is eventually served. Not all officials who break the law get caught; they never did before the PATRIOT Act was passed. No system is perfect and

law enforcement officials continue to refine the best there is to offer. Who will watch these law enforcement officials who, as implied by Epic.org, now have all of these new powers to watch every move we make? Without being sarcastic, is this really what Americans think is happening? Is half of our country now working for the government as agents? The answer is no. It is rather amazing that anyone, let alone an organization that has its roots in America, could honestly believe that our law enforcement personnel are free to do with the law as they wish. As stated, some misuse their powers and when caught are brought to serve justice. Reading the newspaper and watching the news does not make a person an expert on terrorism. The critical issue here is at what point those, who know very little about the capabilities and limitations of law enforcement and terrorism, will cease to inject themselves into the subject. The waste of manpower and resources defending what is essential for the good of the people is a crime in itself. There is no problem questioning what the government does; however, there are groups who no matter what the answer is will not accept the truth.

Small town America does not understand that the FBI is not looking to find out what books a teenager checked out, unless of course the books are all about bomb making. Why not question why there are books like these in the first place? Once again we would be impinging on one right or another. Law enforcement agencies are not tracking everything a person buys, unless a person is buying an unusual amount of manure or the components to make a pipe bomb and have checked out the how-to-books. It is unlikely that cameras will line every street and the government will track peoples every move. Helicopters are not flying all over the country snatching innocent people up because these people are committing innocent acts. There is a thought throughout the land that it is nobody's business what one does. Knowing that a neighbor is about to commit an atrocity against society is the business of law enforcement and concerned

citizens. It took an attack on a very large scale to open some eyes. The attack in 1993 was not enough to get all of America concerned. There was no need to legislate any new tools for law enforcement because of a disgruntled Muslim cleric. America has begun to see that Islamic terrorist do in fact reside in the United States of America.

Understanding terrorism and crime is the first step for those who feel our civil liberties are being stripped away. The Electronic Privacy Information Center and other groups are using civil liberties to scare the average American into believing the government already has or is seeking additional powers to watch and track their lives. When these groups understand the threat and what America can and cannot do to protect itself is when they will most likely win more advocates. Informing the public is quite different from scaring the public. The government has an obligation to protect Americans and preempt attacks if possible. The average American will have to decide if the government knowing what book they checked out is more important than when and where the next terrorist attack on American soil will take place.

A majority of Americans may have gotten their first taste of terrorism on September 11, 2001, but citizens of the world know that terrorism did not begin on that dreadful day in American history. Sadly terrorism has a very well known and extensive history that has been documented around the world. Terrorism has been in existence longer than the Constitution of the United States. The Bill of Rights has become an extremely controversial topic since 9/11. The government techniques of investigation, detainments, and prosecution in the name of national security have been challenged and will continue to be, as America continues its attempt to find a balance between liberty and security. The PATRIOT Act is an effective instrument of counterterrorism but the controversy surrounding its use, and misuse, warrants an investigation into alternative security measures. There are a variety of potential scenarios that could unfold

following the removal of the PATRIOT Act from counterterrorism's arsenal. Fortunately, the most likely future involves both the U.S. and our allies increasing their level of inter-continental cooperation and involvement when developing new counterterrorism security policies. Research has demonstrated that national security involves the following: "A successful global strategy against terrorism requires stability and the continuity of cooperative efforts that are bilateral, regional, and multilateral" (Narasimha, R). As former British Prime Minister Tony Blair said in response to the attacks on the U.S. on September 11, 2001, "This is not a battle between the United States of America and terrorism, but between the free and democratic world and terrorism" (Blair). With global cooperation and effort, terrorism can be effectively controlled without violating the civil rights it threatens to destroy. If we as Americans choose to violate our founding principles, we are no better than the terrorists and the methods they use. Our founding fathers were considered treasonous and terrorists of their time. However, they believed in due process and life, liberty, and the pursuit of happiness.

References

Blair, Tony. 2001. Global Mourning. People.com, September 24. Retrieved from http://www.people.com /people/archive/article/0,,20135394,00.html.

(Constitution) The United States Constitution. http://www.usconstitution.net/const.html

(Cornell) Cornell University. Bill of Rights. Retrieved from http://www.law.cornell.edu/constitution/constitution.billofrights.htm

Democratic underground. Appeals court says some Patriot Act provisions unconstitutional (December 2007) Retrieved from http://www.democraticunderground .com/discuss/duboard.php?az=view_all&address=102x3097042

Franck, Thomas M. Criminals, Combatants, or What? An Examination of the Role of Law in Responding to the Threat of Terror. The American Journal of International Law, Vol. 98, No. 4 (Oct., 2004), pp. 686-688. Retrieved from http://www.asil.org/files /EditorialCommentsCriminalsCombatants.pdf.

Gregory, A. Suspected Terrorist Deserve Due Process. Sept 2005. Retrieved from http://www.independent.org/newsroom/article.asp?id=1570

Lithwick, Dahlia and Julia Turner. "A Guide to the Patriot Act, Part I; should you be scared of the Patriot Act." Retrieved from MSN.com. 08 Sep. 2003. http://slate.msn.com/id/2087984/

Macsata, Brandon. The TSA is violating our Fourth Amendment rights Retrieved from http://dailycaller.com/2010/11/30/the-tsa-is-violating-our-fourth-amendment-rights/#ixzz1EMVST5Qk.

Machi, Sara. Attacks Threaten Civil Rights. The Badger Herald. (2001November). Retrieved from http://badgerherald.com/oped/2001/11/25/attacks_threaten_civ.php

McDougall Paul. November 29, 2010. InformationWeek WikiLeaks Fallout: White House Orders Security Clampdown. Retrieved from http://www.informationweek .com/news/security/management/showArticle.jhtml?articleID= 228400135 &cid=RSSfeed_IWK_News.

Narasimha, Roddam and Kumar, Arvind. 2007. Science and Technology to Counter Terrorism: Proceedings of an Indo-U.S. Workshop. Ed. Stephen P. Cohen and Rita Guenther in cooperation with International Strategic and Security Studies Programme of the National Institute of Advanced Studies, Bangalore, India. National Academy of Sciences. The National Academies Press. http://books.nap.edu/openbook.php?record_id=11848 &page=142.

Nimmo, Kurt July 4, 2010 Retrieved from http://www.infowars.com/bp-homeland-security-and-cops-work-together-to-deny-first-amendment/

Purdy, Matthew. Bush's New Rules to Fight Terror Transform the Legal Landscape. The New York Times, November 25 2001. Retrieved from http://www.nytimes.com /2001/11/25/us/nation- challenged-law-bush-s-new-rules-fight-terror-transform-legal-landscape.html.

The United States Constitution." U.S. House of Representatives. 28 Jan. 2005 Retrieved from http://www.house.gov/Constitution/Constitution.html

USA PATRIOT Act. Electronic Privacy Information Center. 01 Nov. 2004. 28 Jan. 2005 Retrieved from http://www.epic.org/privacy/terrorism/usapatriot/

Chapter 5

Public Sector Policy Analysis

"True genius resides in the capacity for evaluation of uncertain, hazardous, and conflicting information".

Winston Churchill

"However beautiful the strategy, you should occasionally look at the results."

Winston Churchill

"A Continuity of Operations Plan is essential for any business or government agency trying to sustain itself in the face of what seems to be an ever-present cycle of disaster."

Amy Fadida

Richard Krueger states an evaluation story is a brief narrative account of someone's experience with a program, event, or activity that is collected using sound research methods." I was surprised not to find many stories relating to the failures during Hurricane Katrina; however I found one that I believe captures the importance of a COOP plan. The following is a true account of man from Louisiana. Due to the length of the original story I have determined the length of the story would have distracted the readers and chose to edit it while retaining the most significant sections that summarize the results of a lack of an effective COOP plan.

The Experience

"I was concerned for my property. I didn't have time to get my important personal and valuable possessions out of my home and there were many reports of people breaking into homes. I saw no law enforcement in the 3 days I was there, or when I returned a few days later. I was appalled when I found out I could not re-enter the city after I had endured the storm and

the first 3 days. I had gas and food but had to leave to look for my mother whom I hadn't heard from. Since phone lines were non-existent, I needed to drive to find her. I later found that she was safe. I spoke with many others in Baton Rouge who felt the same way. Luckily for me, I had friends who were nice enough to help, but most were not so fortunate. Since I saw no law enforcement while in the city, I was wondering where the thousands of military and national guard were and why they were brought in. It would seem to make much more sense to let people in to secure their own property than to send military in.

The power went out during the storm, and then the water came. It would take at least a day before it flooded my home. For the first few hours, the water stayed at the sidewalk area, but then started to rise. Radio reports informed me that the people who manned the generators and pumps were evacuated. They had to be flown back in to get to the pumps. I have never heard of this happening before. Some emergency personnel had volunteered to work the pumps but were refused because they were not certified.

Thousands of military people consumed resources like food, water and electricity that could have been used by residents. I will refer to police and others and emergency services from here on. Emergency services commandeered food, electricity, diesel, and anything they wanted, from wherever they wanted; there was no ability to say "NO," If they wanted it, they took it; they had machine guns. All emergency services took their orders from DHS (Department of Homeland Security). I had a police scanner during the disaster and heard state police say they were treated like "step-children," and that they were to provide security for FEMA, which then was not needed. I have gone through several large storms when local police, fire departments, hospitals and others have worked together on hurricanes, and these people know how to work

together and know the area. There is now an "extra step," Homeland Security, and FEMA whom local have to take their directions from" (Brad).

Evaluating Continuity of Operations: Maintaining a National Continuity Capability at the State and Local Government Level

Introduction

This paper provides an examination into the use of a wide-ranging evaluation system in state and local emergency preparedness and response plans, specifically Continuity of Operations Plans (COOP). This chapter of the Masters Project describes the mixed methods approach that should be utilized. The original proposed memorandum strategy was "Continuity of Operations: planning to ensure an all hazards mission response capability and continuation of essential functions and services." The majority of COOP plans are enormous and to attempt to evaluate all sections of any COOP Plan in this project would be nearly impossible. The Department of Homeland Security (DHS) has an abundant information about "All Hazards" that the United States faces on a constant basis. The intent of this Masters Project is to introduce various methods to evaluate a state or local government COOP plans. Currently there is no mechanism or mandate in place to ensure state and local governments are prepared in the event of a natural disaster or a terrorist threat. COOP plans detail essential capabilities required to support functional areas, address circumstances that may cause a loss of essential capabilities, and assist leaders and staffs to plan for contingencies to maintain recovery mission essential functions and capabilities (HSPD-9). An alternative for disconnected or interrupted services begins with an effective Continuity of Operations (COOP) plan which includes provisions for Disaster Recovery. Utilizing comprehensive evaluations greatly reduces the overall impact of a disaster

by reducing the risks often associated with the most exposed populations and alleviating the fallout after a disaster strikes.

Stakeholders

Performance measurement systems succeed when the organization's strategy and performance measures are in alignment and when senior managers convey the organization's mission, vision, values and strategic direction to employees and external stakeholders. The performance measures give life to the mission, vision, and strategy by providing a focus that lets employees know how they contribute to the success of the company and its stakeholders' measurable expectations. Stakeholder is defined as "individuals, groups, or organizations that can affect or are affected by an evaluation process or its findings" (Wholey, J). Community stakeholder groups can be divided into three different categories: social groups, economic groups, and political groups. In turn, each of these groups can be characterized by its horizontal and vertical associations.

Social groups are private sector groups such as religious organizations and other nongovernmental organizations (NGOs), nonprofit organizations (NPOs), community based organizations (CBOs), and businesses. All of these groups vary in size, level of organizational complexity, and resources available. All are potential allies in preparing emergency management practices and policies (FEMA -S).

Economic groups are businesses that are the fundamental units in the hierarchy of economic stakeholders. Businesses are important stakeholders because they are part of the societal institution that organizes the flow of goods and services. Destruction, damage, and interruption of business activities can have significant adverse effects on the local economy and possibly on a larger scale in smaller counties. An especially important type of business that is a

stakeholder in emergency management is the public utility provider. These include the providers of electricity, water, sewer services, solid waste management, and communications such as telephone, television, and Internet access. They are responsible for rapid restoration of basic services to all their customers (FEMA -S).

Political groups are various types of governmental stakeholders. Beginning at the base, the lowest level of organization is the municipality (town or city) and just above this, the county. These jurisdictions have different levels of power from one state to another because states differ in the powers that they grant to their political subdivisions. Different governmental levels perform equivalent and matching roles, but agencies within each level of government differ in their functions. For example, at the local level of government, the agencies most involved with emergency management are the fire and police departments, which are the first agencies to respond to most emergencies. In many jurisdictions, the emergency management function is attached to one of these departments, but in larger communities it frequently is an independent agency. In some communities there is a separate emergency medical services agency, but often this function is provided by the fire department working together with local hospitals and ambulance companies (FEMA -S).

The most important stakeholders are the state emergency management agencies, which vary widely in their levels of expertise, staffing, budgets, and other organizational resources. Nonetheless, these are the agencies that provide the major direction for local emergency managers, interact with state legislatures to provide the legal framework within which local emergency managers work, and serve to link local governments with FEMA regional offices (Chapter 2).

Discussion

Evaluations determine a program's effectiveness in meeting its intended purpose and producing competent employees. Evaluation is the quality assurance component of a systematic approach to any program. This paper provides information on evaluation instruments used to gather employee, supervisor, and instructor feedback to identify strengths and weaknesses of training programs at the state and local government levels. It should be used in conjunction with an organization Continuity of Operations Plan (COOP). In 2003 Homeland Security Presidential Directive-8: National Preparedness called for establishing a system that would assess the nation's overall preparedness and provide an annual status report of national preparedness. Three years later, the Post-Katrina Emergency Management Reform Act (PKEMRA) included requirements to establish a "comprehensive system to assess, on an ongoing basis, the nation's prevention capabilities and overall preparedness" (HSPD-8).

The key to conducting an effective evaluation is to first identify the questions to be answered by the evaluation. Should the program be modified? What performance gains are being realized? Is the need for training being addressed in the best way possible? The purposes of an evaluation include the following (Wholey, J):

- To determine if a program is accomplishing its objectives.
- To identify the strengths and weaknesses of a particular program.
- To identify which programs benefitted the most, or the least, from a training program.
- To determine if a program was appropriate for its intended purpose and target population.

In the event of a threat to a state or local jurisdiction, emergency management organizations will need to continue uninterrupted essential component functions across a wide range of potential emergencies including localized acts of nature, accidents and technological and/or attack-related emergencies. Each organization or agency will need to prepare a COOP for actions to be taken by all of its government employees (police, public works, emergency services etc.), civilian employees (secretaries, dispatchers, hospital staff etc.) and the civilian population, should an emergency happen which would eventually cause a governmental organization to declare a COOP event. COOP spans three phases:

Phase 1: Activation and relocation (response 0-12 hours). This phase starts at the onset of an unannounced COOP event or when formal declaration is made of an impending COOP event. The COOP must be executable with or without prior notice and during all hours (COOP Training). Actions in this phase include but are not limited to the following:

- Activation of alert and notification procedures
- Deployment and emergency relocation facility (ERF) activation
- Reception, coordination, and establishment or transfer of command and control
- Personnel accountability
- Initiation of procedures and schedules to transfer MEFs, personnel, records, and equipment to an ERF or alternate office, building, space or area

Phase 2: Alternate operating facility (recovery). This phase enables the relocating staff to assume and commence MEF from the ERF. Priority is given to executing MEF, continuing C3I, logistics support, maintenance and restoration of law and order, command, control and communications, damage/residual resource assessment and reporting (COOP Training).

Phase 3: Reconstitution (termination and return to normal operations). Reconstitution actions focus on restoration of command staffs, capabilities, and functions. This includes: restoring essential C4I; restoring or maintaining communications with higher, lower, and other headquarters or agencies, as required; restoring all organizational capabilities and functions; reconstituting the organization (COOP Training).

COOP plans must identify which normal non-crisis missions and functions are performed in an emergency and prioritize them for a specific contingency, as shown below:

COOP Emergency Level 1: Portion of organization/agency business functions affected. The primary facility is operational, but normal business operations are suspended in a room, floor, level or section due to fire, explosion, water or other damage.

COOP Emergency Level 2: Organization/agency business functions affected. The primary facility is closed for normal business activities but the cause of the disruption has not affected surrounding buildings, utilities, or transportation systems.

COOP Emergency Level 3: Organization/agency business functions and surrounding area affected. The primary facility and surrounding buildings/area are closed to normal business activities.

COOP Emergency Level 4: Installation area affected. The installation is closed to normal business activities as a result of a natural disaster or of an actual or threatened terrorist attack using weapons of mass destruction.

The identification and prioritization of MEFs is the foundation of a valid continuity plan. An accurate assessment of essential functions will allow the most efficient use of available personnel and equipment during a crisis. It also allows for streamlining of support services required by priority tasks of MEFs (FEMA).

- Priority A - Must continue without interruption and directly support the priority missions of the HHQ and the organization's own MEFs.
- Priority B - An organization can defer no longer than 48 hours from "N" time.
- Priority C - An agency can defer for no longer than 7 days from "N" time.
- Priority D - May be deferred until the event is over and normal operations are restored.

It is impossible to plan properly for a disaster if the likely impacts of various disruptions on an organization, staff section or activity are unknown. Assessing the impact of an event includes estimating not only the quantitative or economic losses but also the qualitative impact on the organization, staff section or activities ability to operate. Three documents can and will assist in preparing plans.

Homeland Security Presidential Directive-5 (HSPD-5) is a Presidential directive issued February 28, 2003 on the subject of "Management of Domestic Incidents." The purpose is to "enhance the ability of the United States to manage domestic incidents by establishing a single, comprehensive national incident management system."

Homeland Security Presidential Directive-8 (HSPD-8) is a Presidential directive issued December 17, 2003 on the subject of "National Preparedness." The purpose is to establish "policies to strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies by requiring a

national domestic all-hazards preparedness goal, establishing mechanisms for improved delivery of federal preparedness assistance to state and local governments, and outlining actions to strengthen preparedness capabilities of federal, state, and local entities."

Homeland Security Exercise and Evaluation Program (HSEEP) is a doctrine and policy provided by the U.S. Department of Homeland Security for exercise design, development, conduct and evaluation. The terminology and descriptions related to exercises in this document are a homeland security industry application of emergency management concepts and principles. To begin the process of identifying functions within an organization, first the areas of responsibility need to be identified using the mission statement, values, goals and objectives of the organization, and a brief review of operating procedures, rulebooks and legal authorities.

Areas of Responsibility Worksheet

Number	**Areas of Responsibility**
1	
2	
Example	Processing personnel records

For each area of responsibility identified, name the functions performed and provide a brief description of the activities typically completed in the identified function. COOP planners should collaborate with individuals from each division or branch of the organization to ask about the functions they and their coworkers perform on a day-to-day basis.

Functions Performed by Areas of Responsibility Worksheet Number	**Functions Performed**	**Brief Description**	**Essential? Y/N**
1			
Example	Update personnel records	Personnel update records daily, assisting 10-12 customers per day	Yes

Identify Mission Essential Functions (MEF). Senior management and the organization's COOP planner should determine the criteria for selecting MEFs. For example, if other organizations are dependent on a particular function to continue their operations, then the function is probably an essential function. Based on the pre-determined criteria, the COOP planner should go back to the previous list and for each of the functions listed under the various areas of responsibility indicate which ones are considered essential (HSEEP).

Test, Training, and Exercises. TT&E involving COOP capabilities are essential to assessing, demonstrating and improving the ability of an organization to execute their COOP plans and programs. Tests and exercises serve to validate or identify for subsequent corrective action, specific aspects of COOP plans, policies, procedures, systems, and facilities used in response to an emergency situation. Training familiarizes COOP personnel with the procedures and tasks they must perform in executing COOP plans. In all categories, ask a variety of questions, including such things as: vendor and partner agency agreements or relationships; software and supplies/equipment issues; workstation needs; vital records and documents required; and communications with organization and critical customers (COOP Training).

Testing and Exercises

In order to develop an effective emergency management system, local emergency managers must involve the relevant stakeholders in the process which requires coordinating the various groups as emergency operations and recovery operations plans are drawn up and exercised, as well as during an event. There are a wide variety of tools that can be used to evaluate an organization's COOP plan (COOP Training/HSEEP).

Assessments: In the training context, assessment is the leader's judgment of the organization's ability to perform its mission-essential tasks and, ultimately, its ability to accomplish its doctrinal or directed mission. Leaders and managers are responsible for assessing the performance and the training of soldiers two echelons below their unit. Within these echelons, subordinate leaders' evaluations are the basis for a manager's assessment of his/her organization.

Evaluations:

Evaluation is the process used to measure the demonstrated ability of individuals and units to accomplish their commander's specified training objectives. Training evaluations that are executed will provide senior leadership/managers with feedback on the demonstrated proficiency of individuals, staffs, and subordinate agencies against the mission essential functions and training objective tasks, conditions, and standards. State and local governments at this time are not required; however they should use the following evaluation standards to assess their units (Wholey, FEMA):

- Informal Evaluations - AARs/critiques conducted quickly after training
- Formal Evaluations - Dedicated evaluators and scheduled in training plans
- Internal Evaluations - Conducted by the organization undergoing training
- External Evaluations - Planned, resourced, and performed by higher agencies (SEMO,

FEMA, etc.) coordinated with partners outside the normal chain of command.

After Action Review: The after action review is a method of providing feedback to the organization by involving participants in the training diagnostic process in order to increase and reinforce learning. AARs are conducted during training as well as at the end of training events or during recovery. Leaders use formal or informal After Action Reviews (AAR) to provide feedback on all training. Retraining activities or retraining plans are discussed in all formal AARs (FEMA).

Tests are conducted to evaluate capabilities, not personnel. By testing, organizations can tell if the policies and procedures work, as they should, when they should. Testing results should be published and identified gaps should be actively tracked and managed. Testing is critical for: alert, notification and activation procedures; communications systems; vital records and databases; information technology systems; and reconstitution procedures (COOP Training).

The primary purpose of an exercise is to identify areas that require additional training, planning or other resources. Exercise results should be published and identified gaps should be actively tracked and managed. The goals of a COOP exercise are to discover planning weaknesses; reveal resource gaps; improve coordination; practice using the communication network; clarify roles and responsibilities; improve individual performance; improve readiness for a real incident. After personnel are trained, the COOP plan can be tested through one of three types of exercises: tabletop, functional and full-scale (COOP Training).

Tabletop exercises are a simulation activity in which a scenario is presented and participants in the exercise respond as if the scenario was really happening. New information is presented as the situation unfolds, making the participants reconsider their previous decisions

and plan their next actions based on the new information. Typically, a tabletop exercise takes about 2 hours, including the post exercise debriefing (Unit 5).

Functional exercises test a part of COOP activation to be tested independently of other responders. This includes testing communications capabilities and equipment; primary and backup infrastructure systems and services (i.e. emergency power generators); andrRecovery of records, critical information systems, services, and data (Unit 6).

Full Scale exercises (FSE) are exercises as close to reality as possible, testing the organization's total response capability for COOP situations, with personnel being deployed and systems and equipment being tested (Unit 7). Making the COOP Program an externally inspected program will help convey its importance to senior managers and leadership. The best way to highlight program/project "importance" is to make it one that is inspected and REPORTED by an external agency to the organization's leaders. From that perspective, senior leadership needs to make it an inspection type program with a formal grading system (GO/NO GO, Pass/Fail, etc.) with a similar methodology down through subordinate organizational structures.

The following is an example and describes the evaluation criteria for the contingency plan and test methods (FEMA):

(1) Review plans and procedures for the periodic test of the contingency plan.

(2) Review documentation detailing with when and how the contingency plan has been executed.

(3) Review emergency response procedures.

(4) Verify emergency workload priorities. A list of priority work should be established so that important work continues to be done if possible.

(5) Review alternate procedures for processing priority work.

(6) Use alternate procedures to ensure that priority workloads could be satisfied.

(7) Conduct an emergency response drill.

(8) Ensure that the contingency plan contains a valid and current (within 12 months) MOA with a contingency plan site.

(9) Verify contingency plan site hardware/software compatibility.

(10) Verify list of required personnel for deployment to the alternate site.

(11) Ensure adequate facilities and services are available for personnel while operating at the contingency plan site.

(12) Ensure adequate vehicles have been identified and are operational, should the need for deployment arise.

(13) Verify communications arrangements for deployment to the contingency plan site.

(14) Maintain inventory supplies.

(15) Ensure the contingency plan describes policies and procedures to maintain supplies at the alternate site of operations.

(16) Review procedures for maintenance of backup materials.

(17) Maintain inventory backup materials.

(18) Execute the contingency plan.

(19) Review recovery plans.

The charts below are one example of an evaluation process or method for evaluating an organization's COOP plan. Each evaluation will be unique to an agency depending on what the goal of the assessment is designed for (HSEEP/FEMA).

1 Establishment of a COOP

Rating	Item/Description	Comments

Y N	Is a COOP (primary and alternate) POC designated?	
Y N	Does higher headquarters maintain a roster of their subordinate echelon COOP (alternate and primary) POCs?	
Y N	Has higher headquarters published a COOP plan?	
Y N	Does the higher headquarters maintain copies of their subordinate echelon COOP plan?	
Y N	Has the COOP plan been reviewed annually?	
Y N	Have COOP POCs received training on COOP program responsibilities?	

2. Identification and prioritization of MEFs

Rating	Item/Description	Comments
Y N	Have MEFs been identified and prioritized by the organization's leadership?	
Y N	Do subordinate organizations with MEFs develop and maintain their own supporting COOP plans?	
Y N	Have MEFs that are required by contract been identified?	
Y N	Are procedures established for the improvisation or emergency acquisition of necessary resources?	
Y N	Is there a roster of personnel, by position, needed to perform MEFs?	
Y N	Have MEFs been identified that can be performed from home or other locations, if necessary?	

3. Response Planning

Rating	Item/Description	Comments
Y N	Does the plan take into account all threats that personnel, the mission, and COOP are likely to face?	
Y N	Does the COOP maintain compatibility with HHQ plans?	
Y N	Does the COOP plan establish the capability to shelter-in-place essential personnel?	
Y N	Does the COOP plan establish procedures governing succession to office?	
Y N	Does the COOP plan establish emergency delegations of authority?	
Y N	Does the COOP plan establish procedures for the devolution of command and control?	
Y N	Does the COOP plan establish procedures for the safekeeping of vital resources, facilities, and records?	
Y N	Does the COOP plan address contingency procurement/contracting requirements and procedures during a COOP event?	
Y N	Are provisions for redundant communications included in the COOP plan?	
Y N	Are COOP plans reviewed, updated, and validated every 2 years and a copy provided to higher headquarters?	

4. Emergency Relocation Facilities (ERF) Planning

Rating	Item/Description	Comments
Y N	Has the organization identified the capabilities that are required at the	

	ERF/AH to perform MEFs?	
Y N	Have COOP emergency files, vital records, materials, and databases required to execute MEFs at the ERF/AH been identified and provisions for transporting these items to these locations been made?	
Y N	Are inter-service support agreements, MOUs, MOAs, regarding COOP ERF requirements established?	

5. Assessment of Plans

Rating	Item/Description	Comments
Y N	Are there annual testing, training and exercising of COOP capabilities?	
Y N	Do COOP exercises include weapons of mass destruction and mass casualty contingencies?	
Y N	Are there quarterly tests of COOP alerts, notification and activation procedures?	
Y N	Are annual COOP awareness briefings being conducted for all personnel?	
Y N	Is there a COOP training program for personnel?	
Y N	Are exercise lessons-learned/after-action reviews being used to correct deficiencies in COOP plans?	

6. COOP Awareness

Rating	Item/Description	Comments
Y N	Is COOP information being disseminated through multiple means?	

Y N	Are key leaders and personnel with COOP duties trained in their COOP responsibilities?	
Y N	Does COOP awareness training incorporate the postulated threats?	
Y N	Are there COOP training materials readily available for all personnel?	

Conclusion

The Continuity of Operations (COOP) Program insures that the capability exists to continue organization mission essential functions (MEFs) under all circumstances including crisis, attack, recovery, and reconstitution across a wide range of potential emergencies. This includes all planning and preparatory measures, alert and notification actions, response actions, and restoration activities for all hazards, including acts of nature, natural disasters, accidents, and technological and/or attack-related emergencies. It's important to state that before any plan is exercised or evaluated, personnel must be trained so that they know what their responsibilities are and have the skills and knowledge necessary to carry out their tasks. Training encompasses a range of activities, each intended to provide information and refine skills. Basic orientations are usually the first type of training conducted for new employees. They are typically presented as briefings. Orientations are a good way to introduce the general concepts of the COOP plan as well as announcing to the staff their assignments, roles and responsibilities and describing how the COOP plan will be tested and exercised.

Evaluations are conducted to evaluate capabilities, not personnel. By testing, organizations we can tell if the policies and procedures work as they should, when they should. Testing results should be published and identified weaknesses should be aggressively tracked and managed.

References

Brad. Retrieved from http://911review.org/Hurricane_Katrina/. Accessed 25 April 2011

FEMA, Emergency Management Institute. Retrieved from http://training.fema.gov/IS/crslist.asp.

Chapter 2. Retrieved from http://archone.tamu.edu/hrrc/Publications /books/FEMA_book/FEMA_book_in_PDF/FEMACh_2EMStakeholders.pdf

COOP Training: Course Map. Retrieved from http://www.fema.gov/government /coop/index.shtm .

FEMA –S. Stakeholders Retrieved from training.fema.gov/.../Chapter%202%20-%20Emergency%20Stakeholders.doc

(HSEEP), FEMA, Homeland Security Exercise and Evaluation Program. Retrieved from https://hseep.dhs.gov/pages/1001_HSEEP7.aspx.

Homeland Security Presidential Directive 5 (HSPD–5), Retrieved from http://www.dhs.gov/xnews/releases/press_release_0105.shtm. Accessed 3 May 2011

Homeland Security Presidential Directive 8 (HSPD–8), National Preparedness. Retrieved from http://www.dhs.gov/xabout/laws/gc_1215444247124.shtm.

Homeland Security and Technology Division Planning for Government Continuity November, 2003. Retrieved from http://www.nga.org/cda/files/1103CONTINUITY.pdf.

Unit 5: The Tabletop Exercise. Retrieved from http://www.acp-wa-state.org/meetingsdoc /october2007/03%20Tabletop%20Exercise%20 Guidelines%20-20FEMA%20Example .pdf.

Unit 6: The Functional Exercise training. Retrieved from fema.gov/EMIweb/downloads/is139Unit6.doc

Unit 7: The Full-Scale Exercise Retrieved from

training.fema.gov/emiweb/downloads/is139Unit7.doc.

Wholey, Joseph S., Harry P. Hatry, and Kathryn E. Newcomer. Handbook of Practical Program Evaluation, San Francisco, CA: John Wiley & Sons, 2010.

Chapter 6

Lessons Learned from Comparable Government Perspectives

Kenya Foreign Travel Strategic Plan

Foreword

Millions of U.S. citizens travel abroad each year and use their U.S. passports. When you travel abroad, the odds are in your favor that you will have a safe and incident-free trip. Even if you do come into difficulty abroad, you are unlikely to be a victim of crime or violence. Crime and violence, as well as unexpected difficulties, do befall U.S. citizens in all parts of the world. No one is better able to tell you this than U.S. consular officers who work in the more than 250 U.S. embassies and consulates around the world. Every day of the year they receive calls from American citizens in distress. Problems while aboard can range from such issues as arrests, hospitalization and loss of passport. In these circumstances it is in your best interest as well as our organization's interest to call the nearest U.S. Embassy or Consul for assistance.

The terrorist threat shows no sign of abatement. There remain those whose single-minded goal is to attack American interests and destroy our cherished freedoms. This strategic plan will be an integral part of a larger effort whose purpose remains unchanged: to protect our

people, while maintaining our ability to accomplish the mission. The threat of terrorism will remain and continue to evolve. A fundamental objective and primary challenge of our protection program is to continuously improve and adjust to the changing environment that drives the terrorism.

This strategic plan is provided to ensure that all personnel (executive, staff, and families) are briefed concerning threats and informed of individual protective measures prior to initiation of travel outside of the continental United States or its territories or possessions while either in the performance of their duties or on vacation. All department heads and leadership activities will ensure their staff, faculty, contractors, and family members who plan to visit other countries either while on leave or as part of their duties must coordinate with the company's Security Division to schedule briefs for the countries they plan to visit. As part of this coordination, individuals are required to complete a foreign travel form listing destinations and points of contact while in that country.

Strategic Plan Overview

1. Purpose/mandate. This Strategic Plan, issued in compliance with the United States Military Academy at West Point's overall Strategic Plan, will guide the foreign travel program by articulating the Department of Defense goals and performance objectives, and provide a structure to implement and measures to keep personnel safe (Bryson 226).

2. Background. The United States Military Academy at West Point has personnel deployed to all regions of the world for various reasons. The terrorist threat shows no sign of abatement. There remain those whose single-minded goal is to attack American interests and destroy our cherished freedoms. This plan is a collective, proactive effort focused on the prevention and detection of terrorist attacks against personnel and their families, facilities, and

infrastructures critical to our mission accomplishment. It focuses on the personal protective measures and preparation required to defend against and respond to terrorist incidents.

3. AT vision. West Point accepts as a reality the intent of those that would use terrorism as a tool to destroy people, disrupt our mission, and distract us from our responsibilities. West Point acknowledges that it is a symbol of the nation. As such, our facilities, employees and family members in particular, present a target for terrorists. West Point will protect the West Point family and its staff and faculty and provide training to operate in an environment where the potential for terrorism exists (Bryson 226).

4. AT mission. West Point conducts security and education operations to protect the personnel, their families and facilities by deterring, denying and defending against terrorist attacks. It implements contingency plans to mitigate or respond to criminal or terrorist activities directed against personnel or property on West Point (Bryson 113).

5. Intent. Prior to departure provide a comprehensive review of Nairobi, Kenya, information and personal protection measures. Integrate actions designed to prevent terrorist attacks.

6. Concept/mandate. Focus on supporting goals and objectives of the West Point Security program to facilitate progress toward achieving the stated vision and satisfying the intent of reducing vulnerabilities to terrorist acts.

Strategic Goals

This section describes the strategic goals.

a. All military and DOD civilians will receive annual AT awareness training. Personnel traveling outside the U.S., its territories and possessions (on leave, pass or temporary duty) will

receive an AOR update within two months of travel and must have received annual AT awareness training within 12 months of travel.

b. All military and DoD civilian family members 14 years or older must receive AT awareness training within 12 months of travel, on official government orders, outside the United States, its territories, and possessions and permanent change of station OCONUS travel. Failure to complete required training may result in denial of travel.

c. All DoD-employed contractors will be offered, under terms and conditions specified in the contract, annual AT awareness training and an AOR update prior to traveling outside the U.S., its territories and possessions (including temporary duty) within 12 months of travel.

d. All personnel will be informed of any threat and of all appropriate security precautions designed to reduce their vulnerability to threat attacks prior to traveling outside the U.S., its territories, and possessions.

e. Forms of training include: CJCS-approved, Web-based AT Awareness Course or a course conducted by a certified Level II instructor using an approved lesson plan, containing, as a minimum, the following subjects:

(1) Introduction to terrorism

(2) Terrorist operations

(3) Individual protective measures

(4) Terrorist surveillance techniques

(5) Improvised explosive device (IED) attacks

(6) Kidnapping and hostage survival

(7) Explanation of terrorism threat levels and FPCON System

f. Recent AOR update for the area of travel. View AT/FP Awareness Videos on the following:

(1) Individual protective measures.

(2) Terrorist surveillance detection.

(3) Hostage survival techniques.

g. Complete DoD Level I web-based antiterrorism training: https://atlevel1.dtic.mil/at/

h. Receive AT awareness handouts:

(1) Joint Staff Guide 5280, July 98 and Antiterrorism Individual Protective Measures wallet card.

(2) GTA 19–4–3 (Individual Protective Measures), July 97 and GTA 21–3–11, Army Antiterrorism Individual Protective Measures wallet card.

Country Background: Kenya

Official Name**.** Republic of Kenya.

Country Orientation

Photo's courtesy of US State.Gov

Cities: Capital is Nairobi (pop. 2.9 million; 2007 est.). Other cities: Mombasa (828,500; 2006 est.), Kisumu (650,846; 2005-6), Nakuru (1.3 million; 2005-6), Eldoret (193,830; 1999).

Terrain: Kenya rises from a low coastal plain on the Indian Ocean in a series of mountain ridges and plateaus which stand above 3,000 meters (9,000 ft.) in the center of the country. The Rift Valley bisects the country above Nairobi, opening up to a broad arid plain in the north. Highlands cover the south before descending to the shores of Lake Victoria in the west.

Climate: Tropical in south, west, and central regions; arid and semi-arid in the north and the northeast (State.gov).

Country Description: Kenya is a developing East African country known for its wildlife and national parks. The capital city is Nairobi. The second largest city is Mombasa, located on the southeast coast. Tourist facilities are widely available in Nairobi, the game parks, the reserves, and on the coast (State.gov).

Government Type**:** Republic

Chief of State*:* President Mwai Kibaki (since 30 December 2002); Vice President Stephene Kalonzo Musyoka (since 10 January 2008).

Head of Government: Prime Minister Raila Amolo Odinga (since 17 April 2008)

Safety and Security: On August 7, 1998, the names Osama bin Laden and Al-Qaeda came to international attention when suicide bombs simultaneously detonated at the U.S. embassies in Nairobi, Kenya and Dar es Salaam, Tanzania. More than 300 people were killed, including 12 Americans, and an estimated 5000 people injured (see annex).

On November 28, 2002 Al- Qaida launched a bomb attack on an Israeli-owned hotel in Kikambala, Kenya (near Mombasa) in which 15 people were killed. A near simultaneous attempt to shoot down an Israeli charter plane departing Mombasa was unsuccessful. These incidents have highlighted the continuing threat posed by terrorism in East Africa and the capacity of terrorist groups to carry out attacks. U.S. citizens should be aware of the risk of indiscriminate attacks on civilian targets in public places, including tourist sites and other sites where Westerners are known to congregate (MCIA).

Political demonstrations can occur sporadically throughout Kenya. Travelers should maintain security awareness at all times and avoid public gatherings and street

demonstrations. Violence, including gunfire exchange, has occurred at demonstrations in the past (MCIA). These tend to occur near government buildings, university campuses, or gathering places such as public parks. Police are generally unable to properly manage large demonstrations and they often resort to excessive force to break up large crowds. Most major tourist attractions, particularly outside Nairobi, are not generally affected by protests. However, tribal conflict in rural areas has been known to erupt into violence (MCIA).

Cross-border violence occurs periodically. The area near Kenya's border with Somalia has been the site of a number of incidents of violent criminal activity, including kidnappings. U.S. citizens who decide to visit the area should be aware that they could encounter criminal activity. While foreigners are generally not targets of this type of violence, insecurity in these areas during such times usually increases, placing constraints on travel and threatening the safety and security of travelers in the immediate area. A number of incidents have also occurred near the game parks or lodges north of Mwingi, Meru, and Isiolo, which are frequented by tourists. The U.S. State Department for these reasons, urges U.S. citizens who plan to visit Kenya to take basic security precautions to maximize their safety. Travel to northern Kenya should be undertaken with at least two vehicles to ensure a backup in the case of a breakdown or other emergency (State.gov).

Travel Security

Highway banditry is common in remote and unpopulated areas such as the northeastern province, significant portions of the eastern province, and the northern part of the Great Rift Valley province. Night travel outside major cities is not recommended because incidents occasionally occur on the Nairobi-Mombasa Road. The Kenya Wildlife Service and police have strengthened security in affected areas, but banditry still occurs, especially in and around the

national parks and game reserves. Travelers who do not use the services of reputable travel firms or knowledgeable guides/drivers are especially at risk. It is best to travel in vehicle pairs in order to ensure a backup is available in case of mechanical failure or emergency. When traveling along Kenyan roads, one also has to take into account the poor road conditions and the unpredictable driving habits of the local population (State.gov/MCIA).

In addition, crime is high in all regions of Kenya, particularly Nairobi, Mombasa, Kisumu, and at coastal beach resorts. There are regular reports of attacks against tourists by groups of armed assailants. Pickpockets and thieves carry out "snatch and run" crimes on city streets and near crowds. Visitors have found it safer not to carry valuables, but rather to store them in hotel safety deposit boxes or safe rooms. However, there have been reports of safes being stolen from hotel rooms and of hotel desk staff forced to open safes. Walking alone or at night, especially in downtown areas, public parks, along footpaths, on beaches, and in poorly lit areas, is dangerous and discouraged (State.gov/MCIA).

On May 1, 2011 the U.S. Department of State released this alert: “U.S. citizens traveling and residing abroad [for] the enhanced potential for anti-American violence given recent counter-terrorism activity in Pakistan. Given the uncertainty and volatility of the current situation, U.S. citizens in areas where recent events could cause anti-American violence are strongly urged to limit their travel outside of their homes and hotels and avoid mass gatherings and demonstrations. U.S. citizens should stay current with media coverage of local events and be aware of their surroundings at all times. This Travel Alert expires August 1, 2011.” This alert was a result of the capture and killing of the Al-Qaeda leader Osama bin Laden.

Prior to Departure

1. This information can be found at State.gov. on the most recent travel advisories for any location of your travel. You should visit the Department of State web site at http://travel.state.gov and may also want to contact the Department of State recorded messages at 202-647-5225.

2. Carefully complete your visa application, as it will be scrutinized. If you are a naturalized U.S. citizen returning to the country of your origin, your citizenship may be questioned. If you encounter such a problem, please contact the State Department for guidance.

3. Ensure that items you carry with you are not controversial or prohibited. Political material or anything that could be considered pornographic should not be carried. If you carry prescription drugs with you, be certain that they are clearly marked and bring only necessary quantities.

4. Carrying letters, packages or gifts to individuals in other countries should be avoided as you may be viewed as a courier attempting to bring the material for subversive or illegal purposes.

5. Limit the amount of identification that you take. If you have several forms of ID, bring only one. Make a photocopy of any ID or credit card you will be bringing to leave at home. Write down your passport number and keep it separate from your passport. Do the same with your address and telephone.

6. Contact the American Embassy or Consulate prior to your arrival, and provide your local address and the probable length of your visit.

7. Use of public transportation is recommended rather than driving yourself. Taxis are the preferred mode of transportation. State Department travel advisories provide updated information regarding public transportation concerns in the country you are visiting (State.gov).

8. Before your departure, it is recommended that you provide your family and/or a close friend with the name and phone number of your supervisor or coworker so that you can be reached in the event of an emergency. If this is not possible, the 24 hour State Department Operations Center at 202-647-1512, may be able to assist others in reaching you.

9. To avoid being a target, dress conservatively. Carry the minimum amount of valuables necessary for your trip and plan places to conceal them.

10. Keep medicines in their original, labeled containers. If a medication is unusual or contains narcotics, carry a letter from your doctor attesting to your need to take the drug.

11. Pack an extra set of passport photos along with a photocopy of your passport information page to make replacement of your passport easier in case it is lost or stolen.

Personal Protection Measures, Activities and Behavior

All travelers should learn about the customs, culture, history and geography of the area to which the DoD member has been assigned or is visiting. This should include learning at least a few phrases in the country's language for use in emergencies. Know how to ask for the police or medical care. Consider carrying small cards with emergency phrases on them. You may even consider making cards with pictures or international symbols you can point out to communicate your needs. Make changes to vary your routine. Change your route to and from work and vary your departure and arrival times. Change the times and places for your daily exercise. Enter/ exit buildings through different doors, if possible. Don't allow yourself to be predictable (AT Level I).

1. In all of your activities, show discretion and common sense. Maintain a low profile. Refrain from any behavior that may make you conspicuous or a potential target. Never engage in any illegal activity, excessive drinking or gambling. Use your best judgment to carefully avoid

any situation which may allow a foreign intelligence agency the opportunity to coerce or blackmail you, or criminals to take advantage of your situation (AT Level I).

2. If you locate any possible surveillance equipment, such as microphones, telephone taps, miniature recording devices, or cameras, do not try to neutralize or dismantle them. Assume the device is operable and that active monitoring is ongoing. Report what you have found to the U.S. Embassy or Consulate (AT Level I).

3. Foreign intelligence services may place you under physical surveillance or you may suspect that you are being watched. It is better to ignore the surveillance than attempt to lose or evade it. In any event your actions should be prudent and not likely to generate suspicion. Good precautionary measures are to use well traveled highways and avoid establishing routine schedules (AT Level I).

4. Never try to photograph military personnel, installations, or other "restricted areas." It is best to also refrain from photographing police installations, industrial structures, transportation facilities and boarder areas (AT Level I).

5. Beware of overly friendly or solicitous people. Do not establish personal or intimate relationships with these individuals as they may be employed by the intelligence service. Do not share any work related information with any person who does not have a need to know (AT Level I).

6. If you will be on an extended visit and expect to be writing or receiving mail, remember that it may be subject to censorship. Never make references to anything you don't want read or confiscated.

7. Avoid any areas where there is political or ethnic unrest, demonstrations or protests.

8. Should you be detained or arrested for any reason by the police or other officials, be cooperative and contact the U.S. Embassy or Consulate immediately. Do not make any statements or sign any documents you do not fully understand until you have conferred with an Embassy representative (State.gov).

9. Do not leave documents in hotel safes.

Awareness on the Street

a. Maintain a low profile; dress and behave in public in a way that "blends in" with local customs (AT Level I).
b. Avoid clothing that makes you stand out as a foreigner. Avoid clothing with U.S. flags, logos, etc. (AT Level I, [see photos]).
c. Don't flash large sums of money, expensive jewelry or luxury items. Standing out as an American makes you a target (AT Level I).
d. Be sensitive to local standards of behavior; for example, in some countries a public display of affection is inappropriate (AT Level I).
e. Be alert to your surroundings; stay out of areas that are hostile and unlighted streets, mob-type crowds; think crowd prevention (AT Level I, [see photos]).
f. Watch for unexplained absence of local citizens. Sometimes this can be an early warning of possible terrorist actions (AT Level I, [see photos]).
g. Watch for suspicious parcels, packages or objects that seem to be out of place. An improvised explosive device can look like almost anything: a briefcase, a lunchbox, a shopping bag. Trust your instincts and if it doesn't feel right to you, don't touch it. Report it to the nearest official.
h. Watch for suspicious vehicles. Improvised explosive devices have been placed in

automobiles, bicycles and trucks. They may be parked on the road, or driven to a target location. The driver may abandon the vehicle and jump into an escape vehicle. Get away quickly, sound an alarm if appropriate, notify authorities (AT Level I).

i. Look for signs that you are being followed or watched. Watch for subtle changes in people who you see repeatedly, or two different cars with the same driver.

j. Surveillance can be confirmed by changing directions or making several turns, whether you are in a vehicle or on foot. Retrace your course; use windows and mirrors to look behind you. Make unexpected stops. Vary your pace and trust your instincts. If you confirm that you're being followed, or even feel strongly that you may be under surveillance, don't go home. Conceal your suspicions and go to a safe haven and report the incident. Do not confront the individual(s), as you do not know their intentions, how many there are or if they're armed (AT Level I, [see photos]).

Terrorist Threat

Terrorism is a criminal act committed for political, religious, or ideological reasons. Explosive bombing is the most commonly employed terrorist tactic worldwide and kidnapping is the second. Immediately upon notification of deployment into a high-risk area, determine the terrorist threat for that area. Gather as much information as possible on terrorists and terrorist activity in the area from your security or intelligence officer, libraries, newspapers, magazines, books, people who have been or are now in that area, Department of Defense (DoD) schools that conduct terrorism training, or any other available sources. Once in country, continue to obtain information from the U.S. Embassy, the U.S. Military Group (MILGP), your S2 and the internet. It is imperative that this information and changes in the threat be disseminated to the lowest level (AT Level I).

In most cases, terrorists will seek to attack a target that is unprotected and that will guarantee the most media coverage worldwide. Media coverage of any terrorist incident serves to inflate and distort the public's perception of the terrorist, making him larger-than-life rather than showing him for what he really is, a criminal. To begin a general terrorist threat assessment for your organization, address the following questions:

(1) Do violence prone groups exist in your geographic area of interest?

(2) If you or your organization were attacked by terrorists, would the incident conceivably receive wide media coverage?

(3) Can visitors, deliverymen, mailmen, and others gain access to your facility?

(4) Is your existing security limited to an ID badge, a fence or a uniformed guard at the building door?

To begin a general terrorist threat assessment of your personal vulnerability, address the following questions:

(1) Are you a publicly recognizable member of your organization's management or technical team with an assigned parking space?

(2) Do you normally drive or ride in a "prestige" automobile or display a special license plate?

(3) Do you drive the same route between home and work each day, arrive at the same time each day or buy your gasoline at the same station?

(4) In the past 18 months, has your name or photograph appeared in any newspaper, magazine, trade journal or organizational publication?

(5) Do you, or members of your family, engage in a regularly scheduled recreation or

fitness program such as jogging, swimming, golf, tennis, or handball which is usually conducted weekly at the same location?

If you answered "yes" to two or more of these questions, it is a pretty good indication that a terrorist would have little trouble identifying you, following you home, or keeping you under surveillance. You are not a "low profile" person. It might be prudent for you to take increased notice of your surroundings and people as you move through your day. Consider these observations:

(1) Is someone watching your home?

(2) Is your car being followed?

(3) Has your office received recent inquiries about your plans?

(4) Have you noticed anyone taking photographs near your home, car, or office?

(5) Have you seen strangers in the parking lot?

(6) Has a meter reader, building inspector, or repairman visited you recently?

Any of these observations could be indications of possible terrorist targeting. As preventative measures, try to be more conscientious about what is going on around you as this is an excellent self-protective action. Try to develop a new habit of self-protective curiosity. Don‘t be predictable in your daily activities.

1. Eliminate routines:

a. First, and most important of all, honestly examine the existing patterns associated with your day-to-day life. Do you leave home for the office at the same time every morning? Do you drive the same route each day? Do you park in the same space, use the same door, or eat in the same restaurant?

b. Routine habits can be deadly. Repetitious day-to-day routines can do more to make you a terrorist target than any other activity. Terrorists rarely attack people who do not have rigid daily habits, simply because they cannot accurately prepare their trap. Remember that same time + same route + same place = tempting target.

2. Office building security:

a. Many security precautions are simply the application of common sense and are not costly. Be alert to anyone loitering near your office building. Avoid working late on a routine basis. Avoid routinely going into the office on weekends when nobody else is there (AT Level I).

b. Do not clutter building lobbies with plants, displays or art objects that could conceal the presence of a suspicious package or object. Do not place pictures of personnel in the lobby or put their names on the building directory. Avoid listing personnel by name/rank/title in telephone books or rosters (AT Level I).

c. Limit public access to your building. Ground floor offices are especially vulnerable. Do not place desks near the windows. Keep the window blinds closed to prevent observation from outside. Do not place name signs outside offices. Restrooms should be locked as should all maintenance closets, electrical and telephone rooms. Keys should be inventoried and issued on a very restricted and controlled basis (AT Level I).

d. Instruct secretaries not to provide any information on travel plans, dates of departure, airlines, hotels, and so forth to any caller. Do not convey over the phone the absence of personnel in the office. The secretary or receptionist should state that the requested person is in a meeting and obtain the caller's phone number for call back purposes (AT Level I).

e. Impress upon all employees that they should be alert to unfamiliar personal deliveries. Particular attention should be directed at packages left behind, boxes or briefcases in lobbies, restrooms, stairwells, and coffee shops (AT Level I).

f. When hiring, have a police security background check completed on all local employees.

g. Develop, implement, and practice regularly scheduled drills to cope with fire, bomb threats, and intrusion. Establish notification instructions for emergencies such as accidents, kidnappings/hostage taking, or violent intrusions.

h. Limit normal visitor entry and exit of the building to one or two well marked, clean, lighted doorways. Place a security reception desk at each entrance. Equip the desk with a receptionist, telephones, a visitor's log, perhaps a paging system and an emergency alarm warning system. Require employees to escort their visitors when they are inside the building and to stop and offer escort assistance to anyone who is not an organization employee.

i. Have all packages and mail/sent to a centralized point rather than allowing messengers and delivery personnel to wander around the building.

j. Instruct janitors and maintenance personnel to keep their area doors closed and locked except when in use. Move dumpsters 25 feet away from outside building walls and create a 3-foot wide clear space free of bushes, flower boxes, and debris around the outside face of the building.

k. If you have facility areas that are fenced, ensure that the fence is in good repair, gates are locked, and the fence line is not overgrown with brush, weeds, or grass. Inspect and improve nighttime fence lighting, if needed (DoD 2000.12).

l. Good housekeeping practices applied to your building, its entrances, grounds, and parking lot act as a deterrent to attack. A clean, neat, uncluttered, businesslike appearance sends the

terrorist a "message" that the people inside are not negligent, careless or sloppy. Your office or home environment tells the terrorist that you have a security program. Terrorists prefer to attack unprotected and unconcerned targets (AT Level I).

3. Security en route:

a. Many attacks directed against personnel occur when they are transiting between their homes and their offices. Specifically these attacks occur while:

(1) Walking to an automobile.

(2) Traveling in an automobile.

(3) Walking from an automobile.

b. The key to minimizing personal vulnerability to kidnap, hostage-taking, assassination or other forms of attack is simple; avoid repetition and habit patterns during these high threat movement periods. Vary time of departure and arrival from day to day. Do not transport personnel in attention attracting "prestige" vehicles. When traveling in an automobile keep the windows closed and the doors locked. Park vehicles off the street and under cover at night. Lock cars no matter how short a time they may be unattended (AT Level I).

c. Install an alarm system on the automobile and test it daily. Before entering the vehicle look underneath and all around it to be sure that no suspicious objects, strings, wires, or devices have been attached. If you find anything suspicious, immediately notify authorities; take no actions other than moving to a safe location away from the vehicle (AT Level I).

d. Remember that terrorists usually watch potential targets for days before they attempt an attack. Before leaving your home or office, spend a few minutes looking around the street. Are there any cars, trucks, vans, or motorcycles that look out of place or that seems to be "waiting" at the curb, particularly near your home. As you drive, watch your rear view mirrors and take note

of any vehicle that may be following you. If you think you are being followed make two right turns and go back where you came from or pull into a safe haven (AT Level I).

e. Safe haven is defined several ways (DoD 2000.12):

(1) It can be any place along your route of travel where you could go and where terrorists probably would not follow, such as a police department, firehouse, military base, factory gate, etc.

(2) At home or in the office it is normally a strong, secure room or closet containing essentials to sustain life for a limited time plus communications to call for assistance.

f. When driving, use main roads and avoid secondary roads as much as possible. Drive your vehicle in the lane closest to the centerline. This makes it more difficult for attackers to force you to a stop or off the road (AT Level I).

g. Keep at least one-half car length of empty space in front of your vehicle when stopped at traffic signals and stop signs. This gives you room to maneuver your car if you need to escape a kill zone or kidnap attempt. Keep your car in gear ready to move and keep your hand on the horn. Watch what is going on around you, particularly to your rear. If individuals on foot move toward your vehicle, rev your engine and rock or jerk your car forward and backwards in the space you have available. Blow the horn to attract attention. Get out of there even if it means hitting the attackers around your car. Notify the authorities immediately (AT Level I).

h. Select three to five different travel routes from home to office and use a different route each time you travel. Be careful not to use the same routes on particular days. Watch that you do not fall into the habit of using a favorite route more than others. Avoid all detours and do not stop for people in distress as both are commonly employed traps (AT Level I).

i. Do not gas up at the neighborhood service station. Stop at different well-lighted stations along your various travel routes. Keep your fuel tank at least half full (AT Level I).

j. When you are walking to and away from your vehicle, especially between your residence and your vehicle, you are at the greatest period of vulnerability and risk. Be observant, alert, aware of your surroundings and very careful. Develop these skills into new personal protection habits (AT Level I).

4. Security at home:

a. Both criminals and terrorists consider the home a tempting target. Some common sense precautions will help to deter both (AT Level I).

b. Do not advertise where you live. Take your name off the mailbox and the front door. Do not have department stores, dry cleaners, or grocery firms deliver to your home (AT Level I).

c. Do not pose for newspaper photographs at social, business or sports events. Keep a very low public profile (AT Level I).

d. Park your car inside a garage, not on the street. Keep the garage locked at all times.

e. Install a peephole device on all entrance/exit doors so that visitors may be observed. It is also a good idea to install a two-way communication system at the doors. All outside doors should be solid wood or metal with no glass. Deadbolt locks should be installed on exterior doors. Doorways should be well lighted by at least two separate fixtures. Sliding glass doors and French doors should be secured with anti-entry bars and locks (AT Level I).

f. Ground floor windows and upper story windows accessible from balconies, trees, or low roofs should be fitted with iron grills. Keep all window curtains and blinds tightly closed after sundown. It is also a good idea to coat all ground floor windows with mirrored plastic film which

makes the glass much more difficult to break or cut and limits daytime viewing into the house. Mylar shatter-resistant window film is one of several choices (AT Level I).

g. Install a quality burglar alarm system that has an exterior horn or siren and ask your neighbors to call the police if it should sound. Consider running a buried private telephone or intercom line to a neighbor‘s house so that you can call for assistance even if the terrorist cuts your phone lines (AT Level I).

h. Home security should be discussed with all family members. Do not frighten them, but honestly discuss their safety and security and establish procedures for how the door is to be answered and what is discussed over the telephone. You should assume that someone is listening to all your telephone conversations and you should never discuss family travel plan, pickup points, or appointments on the telephone (AT Level I).

i. Do not let anyone into your home to make an emergency phone call. Keep them outside and make the call for them.

j. If you have children, they should be escorted to and from school and school authorities should never release children to any person who is not a family member. Do not permit children to use public transportation or taxis. Spouses should shop in groups of three or more. All family members should be careful not to establish fixed recreation or fitness habits such as tennis every Tuesday and Saturday, or jogging every day at 6:00 AM, etc (DoD, O-2000.12-H).

k. If your residence requires servants, have a background check made before they are hired and consult their references thoroughly. Instruct servants not to provide any information to callers about the family or its activities, and not to allow anyone (including persons in police uniform) to enter the house without the permission of an adult family member. If a servant calls in sick, do not accept the temporary services of a cousin or brother. Plan and regularly hold

family drills for emergency situations such as fire, the burglar alarm sounding, or forced entry (AT Level I).

(l) While these security suggestions may sound frightening and restrictive, the lifestyle changes and discomfort associated with them is far less than that associated with the victimization, kidnap, injury or death of a family member. The person most interested in your continuing safety should be you (AT Level I).

5. Actions if involved in a kidnapping:

The probability of anyone becoming a hostage is very remote. However, as a member of the Armed Forces, you should always consider yourself a potential hostage or terrorist victim and reflect this in planning your affairs, both personal and professional. You should have an up-to-date will, provide next of kin with an appropriate power-of- attorney, and take measures to ensure your dependents' financial security if necessary. Experience has shown that concern for the welfare of family members is a source of great stress to kidnap victims. Bomb threats, actual bombings, and kidnap or hostage incidents are terrorists' most common tactics. No one plans to be on the receiving end of a terrorist attack, but if you suddenly find yourself involved in an incident, thinking about what you would do in advance can help you to react quickly and correctly while avoiding foolish mistakes or panic. Consider the following example (DoD, O-2000.12-H):

a. As you step out of your car, you are suddenly confronted by three armed men in ski masks. Don't struggle or attempt to run. Physical resistance, verbal banter, or sarcastic remarks at this point may lead to physical abuse or death. Remember that the attackers are also scared, uptight and may react violently and irrationally to any provocation. Listen to their instructions and quietly do what you are told (AT Level I).

b. After the first few moments or while you are being driven away from the scene, quietly let your attackers know of any medical problems you may have. It is important that you let the terrorist know immediately if you have a heart condition, diabetes, or allergies; they may intend to drug you or give you an injection to keep you quiet.

c. Force yourself to be calm and keep your brain alert. Make mental notes about your captors, their speech patterns, mannerisms, physical characteristics, those in charge, the type of vehicle, where you are going, landmarks, time, speed, and distance. Try to draw a mental map. Note any distinctive sounds such as trains, airplanes, heavy traffic, horns, bells, construction, and any special odors you may encounter. Use your eyes, ears, nose and brain (AT Level I).

d. Later on, try to establish some measure of rapport with your captors at the same time maintaining your dignity, poise, and honor. Listen to the questions they ask and think very carefully before you answer. Do not lie, but do not volunteer any information and do not discuss the probable reactions of your organization, family, friends, or the authorities. Do not discuss your organization‘s security arrangements, emergency plans, ransom payments or your financial wealth. Do not discuss politics, race, religion, or ideologies (AT Level I).

e. Try a few legitimate complaints on your captors and note their reactions. Complaints relating to the quality of the food, lack of physical cleanliness, need for medication, exercise, or reading material are legitimate. Keep your mind constantly occupied and establish daily routines so that you always have something to look forward to. Exercise daily and closely monitor your own physical and mental health. Many American prisoners of war in Korea and Vietnam found that reestablishing contact with religion sustained them through hard times and captivity and made solitary confinement easier to bear (AT Level I).

f. Kidnap or hostage victims rarely have the opportunity to overpower their guards or to escape. No attempt to escape should be made unless it has been carefully planned in conjunction with a real, not imagined, opportunity. Escape should be attempted only by a person who has the physical skills and mental discipline necessary to ensure the best possible odds of success. The majority of kidnap or hostage victims are eventually released unharmed and resume normal lives. While being held captive, remember that there are many talented and courageous people working to obtain your release; be patient and have faith.

6. Actions for bomb threat incidents:

a. Dealing effectively and safely with bomb threat incidents and actual bombing attacks requires being prepared. A simple, practical, and exercised bomb threat response plan will allow personnel to know what to do in an emergency (DoD, O-2000.12-H).

b. The use of a simple form and a few minutes of instruction will permit any organization to effectively handle telephone bomb threats, real or hoax. A telephone bomb-threat form provides for the organized capture of all available threat information. A good bomb threat response plan and some personal training will help to allay fears and avoid dangerous mistakes in judgment during emergency situations (DoD, O-2000.12-H).

c. Normally, it takes less time to search a bomb-threatened building than it takes to totally evacuate it. Plan for effective searching in conjunction with bomb threats. Also plan for evacuation, but remember to thoroughly search all stairways and evacuation routes before they are employed since the bombs may be hidden under the stairs (DoD O-2000.12-H) .

d. When a suspicious object or item such as a briefcase is found, notify the authorities immediately. Senior personnel responsible for the building should consider evacuation of

personnel. Do not approach or touch a suspect item unless you have been professionally trained in recognition techniques (DoD O-2000.12-H).

e. Should a bomb explode outside the building, do not rush to the window to see what happened. Quickly step into the hallway and remain there a few minutes. There could be a second explosion and if you are standing at the window you could be injured.

f. If you are on the street when a terrorist bomb explosion occurs, quickly get inside the nearest building and remain there. Shattered glass and windows popped out of the frames in high-rise buildings can fall and scythe through the air for blocks around the point of explosion. Never be curious and move toward an area where a bomb has exploded. There may be a second bomb nearby timed to detonate a few minutes after the first (DoD Directive 2000.12).

g. Unless you are qualified to do so, leave medical treatment to experts. You will probably be of greater assistance simply by leaving the scene and reducing the congestion and confusion (DoD Directive 2000.12).

h. Establish a policy that requires individuals who receive packages to come to the building's central delivery point, physically verify that the particular item is expected or ordered and that the sender's return address is known. Instruct family members not to accept or open any small packages delivered to your home unless they know the sender and expect the package. If any doubt exists about a book mailer, large manila envelope or fat letter, call authorities and request that it be examined. Be extra careful about delivered packages during holiday periods (DoD Directive 2000.12).

i. Never submerge a suspicious package in water; place it outside in a shaded area that is dry and free of debris, keep everyone away from it and call authorities (DoD Directive 2000.12).

References

Army Regulation 525-13, “Antiterrorism,” September 2008

Ask.com. New American embassy in Nairobi [page – 7] Kenya. http://images.ask.com/pictures?l =sem&o=15142&q=new% 20american%20embassy%20in%20nairobi %20kenya &qsrc=8&qid=03A773AA07376607C662766674B38412& pstart= 115&page=7

Ask.com. Fast Facts: Terrorism – U.S. Embassy Bombings http://americanhistory.about. com/library/fastfacts/blffterrorism5.htm.

AT Level I. Antiterrorism Level I training. https://atlevel1.dtic.mil/at/

Bryson John M., Strategic Planning for Public and Non Profit Organizations, Jossey-Bass, San Francisco, CA, 3rd Edition

Dave’s Travel Corner. 12/30/00 Kenya. http://www.davestravelcorner.com/photos/kenya/

DoD O-2000.12-H, "DoD Antiterrorism Handbook," February 9, 2004

DoD Instruction 2000.16, “DoD Antiterrorism Standards,” October 2006

DoD Directive 2000.12, “DoD Antiterrorism Program,” August 18, 2003

MCIA - Martine Corps Intelligence Activity Baseline reference Documents [CD] Country Handbooks (Unclassified)

OSAC - Overseas Security Advisory Council. Kenya. https://www.osac.gov/Pages/Login.aspx

State.gov. International Travel Information. Retrieved from http://travel.state.gov /travel/cis_pa_tw/cis_pa_tw_1168.html

Surveillance pictures. [Page 5] http://www.google.com/search?q=Surveillance +pictures&hl=en&rls=com.microsoft:en-us:IE-SearchBox&rlz=1I7ADRA_en&prmd =ivns &tbm=isch&tbo=u&source=univ&sa=X&ei=x_ TNTYrlBOvq0QHvjJHlDQ&ved=0CCQQsAQ&biw=1899&bih=790

Annex A-Photos of the American Embassy Nairobi, Kenya

Front of old Embassy

Photo courtesy of Matthew Cassidy

Inside looking out

Photo courtesy of Matthew Cassidy

Back of Embassy adjacent to vehicle bomb

Photo courtesy of Matthew Cassidy

Temporary Embassy after the 1998 Terrorist Attack

Photos courtesy of Davestravelcorner

The U.S. Embassy subsequently relocated outside of the city-center.

New Embassy in Nairobi Kenya 2002/03

Photos courtesy of ASK.COM

Annex B – Personal Protection Measure Photo's

Photos courtesy of DoD

Photos courtesy of DoD

Photos courtesy of DoD

Photos courtesy of DoD

Photos courtesy of DoD

Photos courtesy of DoD

Chapter 7

Threat Assessment

Intelligence Gathering Strategies for Homeland Security

November 2011

Prepared by Matthew J. Cassidy, Installation Antiterrorism Officer, United States Military Academy West Point, New York. The purpose is to identify the current assessment of a potential threat (Active Shooter) against the U.S. Military Academy, its personnel and the Academy's potential vulnerability to those threats.

Identifying Subject Matter

This assessment includes information derived from the U.S. Department of Homeland Security (DHS) (unclassified documents), Department of the Army (DA) (unclassified documents) and open sources. The reliability of the open sources used is assessed at medium

reliability: the information is realistically sourced and credible but not corroborated enough to warrant a higher level of confidence. Information received from the DHS and DA is assessed as highly reliable since the information is credibly sourced and corroborated. Where specific source reporting is not available, this assessment relies upon general reporting on the most likely potential terrorist threats and previous specific threats to facilities.

Identifying the Primary Intelligence Consumer

This assessment is intended to provide outlook and understanding of the nature and scope of potentially emergent threats and to assist the United States Military Academy in developing priorities for protective measures relating to existing or emerging threats to their safety and security. The information cutoff date for this assessment is 1January 2012. According to the CRS report titled Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches dated January 14, 2009 the Homeland Security Stakeholder Community is defined broadly as all levels of government, the intelligence, defense, and law enforcement communities, private sector critical infrastructure operators, and those responsible for securing the borders, protecting transportation, and maritime systems, and guarding the security of the homeland (Randol, M).

Identifying Known Threat

The Department of Homeland Security Office of Intelligence and Analysis (I&A) and the FBI remain concerned over the possibility of an attack on the United States given the demonstrated ability by al-Qaida and al-Qaida affiliated groups to recruit, train, and deploy operatives from safe havens around the world (ABC). The disruptions during the past year indicate that terrorist groups continually seek to adapt their methods to include attack tactics to avoid detection. Neither the FBI nor the DHS is in possession of any credible or substantial indicators of current or near-term attacks

against West Point or adjacent state/federal facilities. The installation remains at FPCON Alpha with additional Bravo measures (DoD I).

The United States will continue to face threats from home grown radicals inspired by Islamic extremist ideology. In the past few years there has been a rise of thwarted attacks planned by groups of self-radicalized individuals who may not have operational connections to Al-Qaida but were influenced by Al-Qaida's message and shared similar grievances. Al-Qaida is spreading this message at ever increasing levels through a variety of media, much of which is directly targeting American audiences. Online jihadist web forums and magazines now publish in American style English and are familiar with American customs (World Watch).

The Mumbai attacks demonstrated how a group of trained and determined attackers with firearms and other portable weapons can do a great deal of damage in a short period of time. Terrorists are becoming more sophisticated in their methods and tactics. Dismounted assaults are often beyond the response capabilities of local security and law enforcement. Incident response operations require sophisticated coordination, real time intelligence, and effective command and control. If security forces fail to neutralize such attacks quickly, they can lead to long-drawn-out hostage situations. The ability to end such attacks quickly depends on the rapid response of security forces, equipment, training, in-place response protocols, and effective communication.

Homeland Security Intelligence (HSINT) is classified and non-classified information that is gathered and possessed by federal, state, or local agencies that: relates to the threat of terrorist activity; relates to the ability to prevent, interdict, or disrupt terrorist activity; would improve the identification or investigation of a suspected terrorist or terrorist organization; or would improve the response to a terrorist act (Randol, M).

The following characteristics are commonly associated with active shooter suspects. The list is compiled from descriptions of past active shooters and is not meant to be a comprehensive list describing all active shooters. Each active shooter situation is unique.

1. Active shooters usually focus on assaulting persons with whom they come into contact. Their intention is usually an expression of hatred or rage rather than the commission of a crime.

2. An active shooter is likely to engage more than one target. Active shooters may be intent on harming a number of people as quickly as possible.

3. The first indication of the presence of an active shooter occurs when he or she begins to assault victims.

4. Active shooters often go to locations where potential victims are plentiful, such as classrooms, stadiums, and theaters. Active shooters may act in the manner of a sniper, assaulting victims from a distance. Active shooters may also engage multiple targets while remaining constantly mobile.

5. Tactics such as containment and negotiation, normally associated with standoff incidents may not be adequate in active shooter events. Active shooters typically continue their attacks despite the arrival of emergency responders.

6. Active shooters are often better armed than the police, sometimes making use of explosives, booby traps and body armor.

7. Active shooters may have a planned attack and be prepared for a sustained confrontation with the police. Historically, active shooters have not attempted to hide their identity or conceal the commission of their attacks. Escape from the police is usually not a priority of the active shooter

8. Active shooters may employ some type of diversion.

9. Active shooters may be indiscriminate in their violence or they may seek specific victims.

10. Active shooters may be suicidal, deciding to die in the course of their actions either at the hand of others or by self-inflicted wound.

11. Active shooters usually have some degree of familiarity with the building or location they choose to occupy.

12. Active shooter events are dynamic and may go in and out of an "active" status; a static incident may turn into an active shooter event.

Identifying the Unknowns

Non-state armed groups are almost invisible. This makes it harder to track their capabilities, let alone to detect their intentions about when and where they plan to stage an assault. Understanding armed groups requires increased and detailed knowledge of their operational characteristics. Some information is available, but much is not. For example, had more been known about the group that perpetrated the Mumbai attacks, perhaps it could have been prevented. Questions leaders should consider when developing an understanding of the threats are: Who are the leaders of the group, their roles, styles, personalities, abilities, beliefs, rivalries, and their insecurities? Who makes up the group, how are members recruited, trained, and retained, as well as whether they are cohesive or riddled with factional divisions? What is the group's organizational infrastructure: funding sources, communications, logistical control, propaganda and media resources, security, and intelligence capabilities? What are the different ideological, political, and cultural codes, beliefs, and cleavages? What are the group's operational doctrine, strategy, and tactics? Are there linkages with other actors?

Threat Identification.

There was no specific threat information concerning terrorist or criminal activity targeting the U.S. Military Academy at West Point. Furthermore, there was no information

concerning an identified threat to any specific military activity within the U.S. at this time. Criminal threat intelligence for this report was collected from the Federal Bureau of Investigation (FBI), the Defense Intelligence Agency (DIA), the Army Counter-Intelligence Agency (ACIA), and the West Point Military Police (2).

The USMA is an institution with very high visibility. It is the symbolic center of development for the leadership of the U.S. Army. In the ongoing war against terrorism, the U.S. continues to target the training sites and development centers of terrorist organizations, particularly the remnants of Al Qaeda and of the former Taliban leadership in Afghanistan. There is considerable potential of a retaliatory attack against the U.S. as the war on terror continues (ABC).

The unknown and most dangerous threat to West Point is the possibility of terrorist attacks from domestic or international terrorist organizations and individuals, specifically an active shooter scenario. Although there is no known specific threat in the immediate area, it is assumed that domestic radicals and cells are conducting persistent target selection, reconnaissance, surveillance, and operational planning.

An active shooter, according to the National Tactical Officers Association, is "one or more subjects who participate in a random or systematic shooting spree, demonstrating their intent to continuously cause serious physical injury or death to others. Their overriding objective appears to be that of mass murder, rather than some other criminal conduct such as robbery, hostage taking, etc. In most cases some type of firearm is used; however, the hostile actor(s) may use any weapon that may be available." A suspect is considered an active shooter if he or she is still actively shooting, has access to additional potential victims and has a willingness to harm others until stopped by authorities or his/her own suicide (DHS).

History of the Threat.

St. Louis, Columbine, Virginia Tech, Northern Illinois University, and Fort Hood, Texas: the tragic news of late has shown with deadly clarity that no sector of society is immune to the possibility of an active shooter incident; the escalation both in the number of active shooter incidents and in the scale of their destruction is cause for concern. Communities and colleges alike are vulnerable. Today's criminals and terrorists are more determined and more heavily armed than ever before, and crisis situations that include active shooters are occurring with alarming frequency in workplaces, educational settings, shopping malls, places of worship, government buildings, and military installations (Rivera, L).

West Point is vulnerable to an active shooter incident perpetrated by a civilian employee, retiree, family member, soldier or cadet, as well as by non-affiliated civilians. The possible cost of such an act is viewed as "major," given the potential for widespread injuries and impact on operations; minimal warning time and unpredictability are factored into the high assessment of potential risk. Lastly, West Point's preparedness for such an incident is viewed as "fair" since readiness and response plans, procedures and capabilities have not been fully validated. It is important to recognize that past hostile intruder/active shooter incidents have shown that, in these situations, there is no time, room or intention for negotiation on the part of perpetrators. The perpetrator is there to cause as much injury as possible in the least amount of time. In most cases, perpetrators use firearm(s) and there is no pattern or method to their selection of victims. These situations are dynamic and evolve rapidly, hence quick action is crucial.

Prevent, Preempt, and Mitigate the Threat

Preparedness and mitigation. Predicting or preventing violence is extremely difficult. Therefore, preparedness and mitigation initiatives serve as a vital part of the risk assessment/risk reduction equation. Appropriate preparedness measures include:

Reliable, redundant, installation-wide warning and communication capabilities. West Point uses a variety of means to notify the installation of an emergency including Giant Voice, a high-powered speaker array that covers the entire installation with voice, tone, and siren warnings; Desktop Alert, a network-centric warning and notification tool which delivers emergency messages via an on-screen message alert window to targeted network users, with the capability to discern by whom and when the message was read; Dialogic Dialer, a computer-based system that automates emergency communications, rapidly sending voice and text messages to all types of devices, including phone, email, and pagers; WKDT, broadcasting on FM 89.3 which can be enlisted to provide emergency information to listeners; and the Command Channel announcements for on-post community telecast and public information (1).

Mutual aid agreements with local, county, and state police agencies. Should installation resources prove inadequate during an emergency, requests will be made for assistance from external emergency services, IAW existing, MOAs or MOUs and resource support contracts.

Trained and equipped first responders and emergency management personnel. Rapid deployment of active shooter response tactics must be simple by design, flexible, easy to implement, and effective against a fast moving and unpredictable suspect. Also, initial first responders should have the authority and the capability to take action without waiting for command directives or the arrival of specialty units (e.g., SWAT or crisis negotiators). The goal of police intervention in active shooter incidents is to neutralize the threat by various means, up to and including the use of deadly force.

Validated emergency response plans. All organizations no matter what size are required to have a fire/bomb shelter in place, and an active shooter plan. Each of those plans is required to be exercised at least once annually

Educated, alert and prepared community. For those individuals (military, civilian, cadets) directly or indirectly involved in the incident, the following protective directives may be employed. Evacuation: when conditions are safer outside than inside a building, all personnel in the hazard zone will be directed to leave the building immediately to a designated safe area. Evacuation of an entire facility or area may not always be prudent, especially if evacuation may lead to other risks by taking the occupants out of the physically secure environment of the facility and onto the streets; Reverse Evacuation: when conditions are safer inside a building than outside, personnel may be directed to seek shelter indoors. Once all personnel are inside, the building exterior doors should be locked and Lock down/Shelter-in-Place procedures initiated; Lockdown/Shelter-in-place: when a person or situation presents an immediate threat to personnel in a building, the order to lock down or shelter-in-place may be given.

Confront the attacker: because active shooter situations are often over before law enforcement arrives on the scene, individuals must be prepared both mentally and physically to deal with the assailant. When the shooter is at close range and you cannot flee, your chance of survival is much greater if you try to incapacitate him/her (DHS).

Additionally the Antiterrorism Working Group Meeting (ATWG) has a representative from each organization that attends. The purpose of the ATWG is to review threats, identify vulnerabilities, recommend countermeasures, recommend force protection condition changes (FPCONs), and monitor corrective actions.

Identifying and Describing the 2008 Mumbai Attack: Attack Summary

The 2008 Mumbai attacks began early in the morning of 26 November 2008 and included sustained operations lasting approximately 60 hours. The ten attackers, members of Lashkar-e-Taiba (LeT), entered the coastal city from the sea by first hijacking a fishing trawler and killing the crew, and then transferring to small boats to minimize their deployment signature. Once ashore, the group divided into four assault teams. The terrorists were equipped with automatic weapons, grenades, improvised explosive devices (IED), satellite phones, Blackberries, and detailed maps and images of the targets (Wax, E). The teams conducted sequential attacks against a railway station, cinema, restaurant, residential complex Jewish Center, hospital, and multiple hotels and taxis. The attackers made deliberate attempts to identify and kill Westerners. By "pulsing" from target to target and by leaving IEDs in taxis, the group was able to increase confusion and minimize response-force effectiveness. Handlers in Pakistan provided live command and control to the terrorists and helped them plan responses to security forces. With support from pre-positioned caches of ammunition and food, the group was able to sustain their assaults and hostage taking operations (Roggio, B). In 60 hours of fighting, 173 civilians were killed and over 300 wounded; one terrorist was captured and the other nine were killed.

The terrorists used two distinctive tactics to carry out their attacks: Tactic 1 Hit and Run: terrorists advanced quickly attacking with AK-47s and grenades, targeting large groups and then retreating from security and moving on to other targets. Tactic 2 Seize and Hold: terrorists gained entry and immediately started firing indiscriminately at groups of people and taking hostages (Roggio, B). Attackers used detailed knowledge of the facility layout to their advantage, selecting additional targets until they established strong-points to defend against security. Details of the 60-hour siege suggest the attackers had planned the attack several months ahead of time and knew some areas well enough for the attackers to vanish and reappear after

security forces had left. Blood tests on the attackers indicate that they had taken illegal narcotics during the attacks to sustain the energy necessary for the continuous 60 hour confrontation (McElroy, D). Questioning of the lone surviving gunman indicated attackers had used a program such as Google Earth to familiarize themselves with the locations of buildings used in the attack.

India's Short and Long Term Response

The police were able to gain control of the situation at the CSP train station, cafe, and cinema fairly quickly, though they were unable to handle the hostage situation at the hotels, the hospital, and the Jewish Center. The Sherman Kent Analytic Doctrine states: "there needs to be a candid Admission of Mistakes" in the Mumbai incident. The police officials admitted they were "overwhelmed" by the attacks and unable to contain the fighting (Roggio, B). Following the Mumbai terrorist attack, Pakistan pledged to the Security Council that it would take action against LeT and its front organization Jamaat-ud-Dawa. The Rand report titled The Lessons of Mumbai identified the issues in the aftermath of the attacks that were considered serious weaknesses with India's homeland security and the ability to mitigate them. These were intelligence failures, lack of coordination, gaps in coastal surveillance, inadequate "Target Hardening," inadequate counterterrorism training and equipment for local police, limitations of municipal fire and emergency services, incomplete execution of response protocols, a flawed hostage-rescue plan, and poor strategic communications and Information management. Looking back to September 11, 2001 India was experiencing some of the same issue that the United States had (Rabasa, A).

Ideology

The Qur'an is central to their ideology**.** LeT subscribes to the strict fundamentalist interpretation of Islam upheld in the Wahhabi theological tradition. Based on this radical

interpretation of Islam, which is closely related to that associated with Al Qaeda, LeT seeks to establish an Islamic caliphate and has declared the U.S., Israel and India as existential enemies of Islam (ADL). “This symbol features a blue circle enclosed by a black border. The center image includes a black AK-47 rifle, placed against a yellow sun that extends vertically from an open, green Qur’an. Above the rifle is a black, semi-circular Qur’anic phrase that reads in Arabic ‘And fight them on until there is no more tumult or oppression, and there prevail justice and faith in Allah.’” The white, Arabic lettering, set against a red background, bears the group’s original name: Markaz al-Dawa wa al-Irshad (the Center for Preaching and Guidance) (ADL).

Principals

Co-Founder and Leader: Hafiz Muhammad Saeed: (Global Jihad 1); *Co-Founder and Chief of Operations and* Zaki-ur-Rehman Lakhvi a.k.a. Abdullah Azam a.k.a"Chacha"(Global Jihad 2).

AQ-affiliation

According to the U.S. State Department, LeT has several thousand members in Pakistan and Kashmir, most of whom are Pakistani and Afghan veterans of the Afghan wars. LeT is also strengthened through collaborations with other terrorist groups comprised of non-Pakistanis and, after a senior Al Qaeda leader was captured in an LeT safe house in March 2002, has been linked to Al Qaeda (ADL).

Modus Operandi

LeT has conducted terrorist operations against Indian troops and civilian targets in Kashmir using assault rifles, light and heavy machine guns, mortars, explosives and rocket-propelled grenades, according to the U.S. State Department. LeT has also carried out several

high-profile attacks against civilian and military targets in India, including suicide bombings and conventional assault tactics (ADL).

Status on the U.S. Department of State's Lists of Designated Foreign Terrorist Organizations and Ties to State Sponsors

Lashkar-e-Taiba (LeT) is listed as number 23 alphabetically not necessarily by threat ranking. They have been designated by the Secretary of State as a Foreign Terrorist Organizations (FTOs); the list was updated in September 2011 (U.S. Department of State 2011).

Sponsors

LeT was established with the aid of Pakistan's intelligence agency, Inter-Service Intelligence (ISI), which also opposes Indian presence in Kashmir. The ISI allegedly provided LeT with funding, weapons, intelligence and instruction in exchange for promising to confine its attacks to Hindus in Kashmir. This financial and logistical support seemingly ended in January 2002 when Pakistan banned the group and froze its assets, following the United States designation of LeT as a foreign terrorist organization the previous month (U.S. Department of State April 30, 2008**,** U.S. Department of State 2008).

Identifying Pre-2008 Attacks

2006 Mumbai train attacks; series of coordinated IED blasts on trains in city

Dec. 2005 attack on the Indian Institute of Science

July 2005 attack on the Ayodhya temple

Dec. 2001 Indian Parliament ttack; targeted Indian politicians in suicide attack on location

March 1993 Mumbai attacks; multiple coordinated VBIED attacks throughout city

2011 Mumbai Terrorist Attacks

On July 13, 2011 three coordinated explosions ripped through Mumbai, India killing 21 and injuring 131 people. The explosions took place during rush hour at the southern Opera House district, in the Zaveri Bazaar jewelry market, and near a transport hub in the suburb of West Dadar, a few miles north of the city center. These areas often attract tourists from around the world and are some of the most crowded parts of the city. Currently no group has claimed responsibility for the attack; however government officials suggest that likely attackers could be the Indian Mujahideen1. The terrorist group claimed responsibility for a series of blasts in various cities across the country in 2008. It is believed to be a shadow organization of the banned Students Islamic Movement of India (SIMI) and Lashkar-e- Tayyiba (English News).

References

1. During the past 5 years the West Point Antiterrorism Officer was able to secure $1.7 million dollars to purchase various types of Antiterrorism/Force Protection and communications equipment to include the Giant Voice, Dialogic, and Desktop alert notification systems.

2. Phones conversations and emails between the Installation Antiterrorism Officer and the FBI, US Army Northern Command, US Army Antiterrorism Intelligence Cell, and personal interviews with the military police and Criminal intelligence Division (CID).

ABC News. Osama Bin Laden: Experts Fear Revenge By Al Qaeda or 'Lone Wolf'. Retrieved from http://abcnews.go.com/US/osama-bin-laden-triggers-security-alert-recall-marine/story?id=13505844

(ADL) Anti-Defamation League. International Terrorist Symbols Database. Retrieved from http://www.adl.org/terrorism/symbols/lashkaretaiba.asp

Bajoria, Jayshree January 14, 2010 Council on Foreign Relations Retrieved from http://www.cfr.org/pakistan/lashkar-e-taiba-army-pure-aka-lashkar-e-tayyiba-lashkar-e-toiba-lashkar--taiba/p17882

DHS - U.S. Department of Homeland Security. Active Shooter How to Respond. Retrieved from http://www.dhs.gov/xlibrary/assets/active_shooter_booklet.pdf

DoDI. Department of Defense Instruction 2000.16 dated October 2, 2006.

English news.cn. July 2011. 21 killed, 113 injured in terror attack in Mumbai. Retrieved from http://news.xinhuanet.com/english2010/world/2011-07/14/c_13983273.htm

Global Jihad 1-Global Jihad. Hafiz Muhammad Saeed. Retrieved from http://globaljihad.net/view_page.asp?id=1252

Global Jihad 2-Global Jihad Zaki-Ur-Rehman Lakhvi. Retrieved from http://globaljihad.net/view_page.asp?id=1257

JedburghCorp. Mumbai Attack Timeline and Order of Battle. Retrieved from http://jedburgh-usa.com/wp-content/uploads/Mumbai%20Reconstruction.pdf

McElroy, Damien. Dec 2008, the Telegraph. Mumbai attacks: Terrorists took cocaine to stay awake during assault. Retrieved from http://www.telegraph.co.uk/ news/ worldnews /asia/india/3540964/Mumbai-attacks-Terrorists-took-cocaine-to-stay-awake-during-assault.html

Pike, John Federation of American Scientists. Intelligence Resource Program. Lashkar-e-Taiba, Lashkar-e-Tayyiba , (Army of the Righteous). Retrieved from http://www.fas.org/irp/world/para/lashkar.htm

Purvis, Carlton Military Threat Level Raised to FPCON Bravo Retrieved from http://www.securitymanagement.com/news/military-threat-level-raised-fpcon-bravo-009004

Rabasa, Angel, Robert D. Blackwill, Peter Chalk, Kim Cragin, C. Christine Fair, Brian A. Jackson, Brian Michael Jenkins, Seth G. Jones, Nathaniel Shestak, Ashley J. Tellis. RAND Corporation. The Lessons of Mumbai. Retrieved from https://blackboard.pace. Edu /webapps/portal/frameset.jsp?tab_tab_group_ id=_2_1&url=%2Fwebapps%2 Fblackboard %2Fexecute%2Flauncher%3Ftype%3 DCourse %26id%3D_98020_1%26url%3D

Randol Mark. Homeland security: intelligence perceptions, statutory definitions, and approaches. Retrieved from http://www.fas.org/sgp/crs/intel/

RL33616.pdf

Rivera Luis. Active Shooter's Incidents. Retrieved from http://www. endesastres.org/files/Active_Shooter_Incident_FINAL.pdf

Roggio, Bill November 2008Analysis: Mumbai attack differs from past terror strikes. Retrieved from http://www.longwarjournal.org/archives/2008/11/analysis_ mumbai_atta.php#ixzz1dPr2pNOL

The Guardian. Tense standoff at Nariman House Retrieved on 1 November 2011 from http://www.guardian.co.uk/world/2008/nov/27/mumbai-terror-attacks-terrorism2

The Telegraph. Mumbai attacks: Pakistan arrests suspected mastermind Zakiur Rehman Lakhvi. http://www.telegraph.co.uk/news/worldnews/asia/pakistan/3681764/Mumbai-attacks-Pakistan-arrests-suspected-mastermind-Zakiur-Rehman-Lakhvi.html

U.S. Department of State April 30, 2008. Terrorist Organizations Country Reports on Terrorism Retrieved on 1 November 2011 from http://www.state.gov/s/ct/rls/crt/2007/103714.htm

U.S. Department of State. Sept.15, 2011. Office of the Coordination for counterterrorism. Foreign Terrorist Organizations. Retrieved from ttp://www.state.gov /s/ct/rls /other/ des/ 123085.htm

Wax, Emily. December 2008. The Washington Post Foreign Service. Mumbai Attackers Made Sophisticated Use of Technology. Retrieved from http://www. washingtonpost .com /wp-dyn/content/article/2008/12/02/AR2008120203519.html

World Watch. September 2011. Al Qaeda magazine celebrates 9/11 anniversary. Retrieved on 5 November 2011 from http://www.cbsnews.com/8301-503543_162-20112927-503543.html

Photo courtesy of Boston.com. Retrieved from http://www.boston.com /bigpicture/ 2008/11/mumbai_under_attack.html

Chapter 8

Civil Liberties and Fundamental Human Rights:

International Human Rights

Adherence to our values is what distinguishes us from our enemy. This fight depends on securing the population, which must understand that we, not our enemies, occupy the moral high ground.

General David Petraeus

Give to every human being every right that you claim for yourself.

Robert Ingersoll

No man is above the law and no man below it.

Theodore Roosevelt

What makes us a great nation is that this is a country that understands that people have God-given rights and liberties. And we cannot—in our efforts to bring justice—diminish those liberties."

Senator George Allen (R-VA)

Introduction

This chapter of my Masters project is designed to combine policy making, security, and human rights into a single dialogue regarding the meaning, policies, role, and purpose of U.S. Homeland Security policy as a response to the threat of global terrorism. To that end, the audiences will not only come away with a better understanding of what Homeland Security is understood to be, but see also how it fits in the wider understanding of security, civil liberties, and fundamental human rights. Particular emphasis will be placed on where the logic of security, liberties, and rights are in conflict or at least require balancing in regards to the threat posed by

terrorism, as well as how understanding of the threat shapes those conflicts and impacts efforts to create an acceptable balance.

Overview

In the past ten years the international community has taken on a new focus when dealing with human rights. Governmental and non-governmental organizations are realizing that some countries take precedent over other countries when it comes to human rights. Cases that violate human rights are being taken more seriously than ever before. International prosecution against individuals has been taking place more frequently than ever; however, I don't believe the conviction rate is sufficient. Human rights are relevant to terrorism as concerns both its victims and its perpetrators. The concept of human rights was first expressed in the 1948 Universal Declaration of Human Rights, which established "recognition of the inherent dignity and inalienable rights of all members of the human family." The innocent victims of terrorism suffer an attack on their most basic right to live in peace and security. Human Rights violations occur all over the world. From disappearances and extra-judicial executions, to the use of torture and police abuse, to violations of the rights to food, housing and health care, human beings are seldom able to enjoy the full extent of their recognized rights.

The issue of Human Rights has occupied the international agenda for a long time, and naturally international relations literature has discussed this issue from different perspectives. Natural rights are understood to be the rights derived from nature and associated with the natural order of things, such as life. Closely related are human rights, which are those basic rights and freedoms that one is endowed with by simply being human. These rights normally include the right to life and liberty, freedom of thought and expression, and equality before the law.

What are Human Rights?

The Office of the High Commissioner for Human Rights (OHCHR) defines human rights as rights inherent in all human beings, whatever nationality, place of residence, sex, national or ethnic origin, color, religion, language, or any other status. We are all equally entitled to our human rights without discrimination. These rights are all interrelated, interdependent and indivisible. Civil rights simply means that people have the right to be treated the same regardless of their race, gender, or religion. These rights are law in the United States as well as many other nations.

According to *Encyclopedia Britannica*, human rights are universal rights held to belong to individuals by virtue of their being human, encompassing civil, political, economic, social, and cultural rights and freedoms, and based on the notion of personal human dignity and worth. Conceptually derived from the theory of natural law and originating in Greco-Roman doctrines, the idea of human rights appears in some early Christian writers' works and is reflected in the Magna Carta (Encyclopedia Britannica). Human rights refer to the concept of human beings having universal rights, or status, regardless of legal jurisdiction or other localizing factors, such as ethnicity, nationality, and sex. As is evident in the United Nations Universal Declaration of Human Rights, human rights, at least in the post-war period, are conceptualized as based on inherent human dignity (United Nations). As Jack Donnelly says, "international human rights policies are one point of national foreign policies which all states consider to be appropriately driven primarily by the pursuit of national interest" (Donnelly, J). When dealing with human rights issues, sometimes the United States will want the help of both parties to a regional conflict and cannot reward one party at the expense of another. A good example of this is with Israel and Egypt. The United States cannot afford to abandon long-standing allies. Such actions will have their own costs and risks. But the United States must be much more disciplined in its choices,

and much more familiar with the views of others, if it is to maintain this coalition over the long term. In the years since the Cold War ended, the United States has been powerful, and relatively impulsive. It has often acted against the interests of others in pursuit of modest gains, as it did in the case of NATO expansion. The existence and the content of human rights continue to be the subject of debate. Legally, human rights are defined in international law and covenants, and further, in the domestic laws of many states. However, for many people the doctrine of human rights goes beyond law and forms a fundamental moral basis for regulating the contemporary geo-political order (Donnelly, J). They see them as democratic ideals.

United States Policy on Human Rights

The protection of fundamental human rights was a foundation stone in the establishment of the United States over 200 years ago. Since then, a central goal of U.S. foreign policy has been the promotion of respect for human rights as embodied in the Universal Declaration of Human Rights (US Department of State). The United States understands that the existence of human rights helps secure the peace, deter aggression, promote the rule of law, combat crime and corruption, strengthen democracies, and prevent humanitarian crises(United Nations). The U.S. State Department believes strongly that the promotion of human rights is an important national interest; the United States seeks to "hold governments accountable for their obligations under universal human rights norms and international human rights instruments; promote greater respect for human rights, including freedom from torture, freedom of expression, press freedom, women's rights, children's rights, and the protection of minorities; promote the rule of law, seek accountability, and change cultures with impunity; assist efforts to reform and strengthen the institutional capacity of the Office of the UN High Commissioner for Human Rights and the UN

Commission on Human Rights; and coordinate human rights activities with important allies, including the EU and regional organizations" (US Dept. of State).

On September 21, 2004 President George Bush spoke to the United Nations General Assembly:

"The United Nations and my country share the deepest commitments. Both the American Declaration of Independence and the Universal Declaration of Human Rights proclaim the equal value and dignity of every human life. That dignity is honored by the rule of law, limits on the power of the state, respect for women, protection of private property, free speech, equal justice, and religious tolerance. That dignity is dishonored by oppression, corruption, tyranny, bigotry, terrorism and all violence against the innocent. And both of our founding documents affirm that this bright line between justice and injustice -- between right and wrong -- is the same in every age, and every culture, and every nation" (White House)

United Nations Declaration of Human Rights

In the aftermath of World War II, many political scientists, social theorists, and notable individuals and diplomats saw the need for a directive type of approach to prevent a repeat of the horrors that occurred in the 1930s and 1940s. From this the United Nations and the Universal Declaration of Human Rights were born. The Declaration attempted to codify rights and freedoms that belong to each human being in the global community.

On December 10, 1948 the General Assembly of the United Nations adopted and proclaimed the Universal Declaration of Human Rights (United Nations-CT), a thirty article declaration that lays out, unequivocally, the fundamental rights of mankind. The second main function was to develop new and effective ways on finding offenders and stopping them. The main focus in this treaty pertains to abolishing slavery and the slave trade. All of the non-

governmental organizations (NGO's) the United Nations, Amnesty, and the Human Rights Watch defend human rights to their fullest extent (Amnesty International). Though most countries have signed the United Nations Universal Declarations of Human Rights, many human rights issues remain unaddressed and unresolved. The enforcement of international humanitarian law is critical not only for the protection of civilians living under occupation, but also in preserving prospects for peace and security. Human rights are frequently held to be universal in the sense that all people have and should enjoy them, and to be independent in the sense that they exist and are available as standards of justification and criticism whether or not they are recognized and implemented by the legal system or officials of a country. Human rights rest upon moral universalism and the belief in the existence of a truly universal moral community comprising all human beings. Moral universalism posits the existence of rationally identifiable trans-cultural and trans-historical moral truths. There is much disagreement about when and to what extent outside countries can engage in human intervention (Donnelly, J).

The purpose of the Office of the High Commissioner for Human Rights (OHCHR), a department of the United Nations, is to promote and protect the enjoyment and full realization, by all people, of all rights established in the Charter of the United Nations and in international human rights laws and treaties (High Commissioner). The mandate includes preventing human rights violations, securing respect for all human rights, promoting international cooperation to protect human rights, coordinating related activities throughout the United Nations, and strengthening and streamlining the United Nations system in the field of human rights (High Commissioner). In addition to its mandated responsibilities, the Office leads efforts to integrate a human rights approach within all work carried out by United Nations agencies.

What is Homeland Security

Terrorists and other violent extremists, particularly those inspired by al-Qaida's violent, extremist ideology, remain focused on attacking U.S. critical infrastructure. Al-Qaida, in particular, has demonstrated an enduring interest in attacking the critical infrastructure of major cities. According to the National Strategy for Homeland Security, homeland security is "a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur." But I think they forgot some of the definition. If you read deeper into the document, it further discusses that Homeland Security is a shared responsibility; it states, "Under the President's proposal, the Department of Homeland Security will consolidate federal response plans and build a national system for incident management in cooperation with state and local governments" (US Government).

The PATRIOT Act

The PATRIOT Act, which allows for the free flow of information between the CIA and the FBI, was passed on October 25, 2001 by a Senate vote of 98 to 1 and a House vote of 357 to 66 (16). In May 2011 the most recent extension of the Patriot Act passed the Senate 72 to 23 and the House 250 to 153 (United Nations-CT) . We no longer feel as threatened, so the level of support is not as high as it was six weeks after the attacks. But it is still, relatively speaking, overwhelming (Davis). The PATRIOT Act (United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) was enacted following the terrorist attacks of September 11, 2001. Its purpose was to expand the authority of U.S. law enforcement agencies to fight and counter terroristic acts. The American Civil Liberties Union has attempted to reverse some of these laws that have been enacted (USA PATRIOT Act). I feel

that current laws that the United States has in place are not sufficient to effectively combat terrorism. In theory, punishment is handed out as a deterrent to prevent future criminal acts. Our laws and the guidelines for punishment were not designed to address national or international acts of terrorism, such as is the case with illegal immigration. With the fact that society and its moral beliefs are always changing and oftentimes quite different, a common ground must be defined that allows our country to fight an enemy that wishes to destroy the foundations of this country, while at the same time providing checks and balances on the government that will provide the necessary protections and prosecutions. Terrorists who are not U.S. citizens that are apprehended on United States soil should not be treated as normal criminals until the laws are changed to deal appropriately with people that wish to cause death and major disruptions to the United States economy. United States citizens that are involved in terrorist acts should be allowed the same constitutional rights as every other citizen until a determination can be reached that they have or were planning terrorist acts. Therefore modification of current law to address terrorism and establishment of better checks and balances on government agencies are needed (USA PATRIOT ACT).

September 11 Detainees

More than 1,200 people were detained in the two months following the September 11 attacks (Office of the Inspector General). The Justice Department classified 762 of them as September 11 detainees, defined as those detained on immigration violations allegedly in connection with the investigation of the attacks (Office of the Inspector General). A 198-page report issued by the OIG in June 2003 makes clear, however, that many of the detainees did not receive core due process protections, and the decision to detain them was at times extremely attenuated. From the focus of the September 11 investigation (Office of the Inspector General)

the OIG finding was that the vast majority of the detainees were accused not of terrorism-related offenses, but of civil violations of federal immigration law. This calls into serious question a recent decision of the U.S. Court of Appeals for the District of Columbia to uphold the Justice Department's decision to withhold the names of the September 11 detainees. The court's opinion relied explicitly on its conclusion that many of the detainees had links to terrorism, and therefore that public access to any of their names could interfere with the government's ongoing efforts to fight terrorism (Office of the Inspector General). The OIG conclusion that the designation of the detainees as of interest to the September 11 investigation was made in an indiscriminate and haphazard manner, catching many aliens who had no connection to terrorism in their net, seriously undermines the basis of the Court of Appeals holding (Office of the Inspector General). Beyond this, the September 11 detainees were subject to a set of Justice Department policies that resulted in serious violations of their due process rights. First, the Justice Department implemented a "hold until cleared" policy under which all non-citizens in whom the FBI had an interest required clearance by the FBI of any connection to terrorism before they could be released. The Inspector General concluded that the clearance process was not conducted in a timely manner: it was understaffed and was not accorded sufficient priority. The OIG reported that the average time from arrest to clearance was 80 days and less than 3 percent of the detainees were cleared within 3 weeks of arrest (Office of the Inspector General).

Second, the Justice Department issued a regulation that increased from 24 to 48 hours the time that the Immigration and Naturalization Service (INS) could detain someone in custody without charge (Office of the Inspector General). Detention without charge could continue beyond this for a reasonable period of time in the event of an emergency or other extraordinary circumstance (Office of the Inspector General). The terms "reasonable period of time,"

"emergency" and "extraordinary circumstance" were not defined. The expanded authority applied even to detainees who were not charged with a crime or suspected of presenting a risk to the community. With the new regulations in place, many detainees did not receive notice of the charges against them for weeks, and some for more than a month after being arrested (Office of the Inspector General). Consistent with early data, the OIG reports that 192 detainees waited longer than 72 hours to be served with charges; 24 were held between 25-31 days before being served; 24 were held more than 31 days before being served; and five were held an average of 168 days before being served (Office of the Inspector General). Further, because INS did not record when a charging decision was made, the OIG concluded that it was impossible to determine how often the INS took advantage of the reasonable time exception to the charging rule (Office of the Inspector General).

Third, the lack of timely notice of the charges against them undermined the detainees' ability to obtain legal representation, to request bond, and to understand why they were being detained. In addition, the Inspector General found that detainees had been prevented from contacting lawyers during a communications blackout at the Metropolitan Detention Center (MDC) in Brooklyn, New York, and detainees' families and attorneys were unable to receive any information about them, including where they were held (Office of the Inspector General). In some cases, attorneys were told that their clients were not detained at MDC when in fact they were. According to the OIG report, the first legal call made by any September 11 detainee held at MDC was not until October 15, 2001. This blackout, in conjunction with access-to-counsel problems created by the charging delays and restrictive legal access policies like that at MDC, seriously impaired detainees' ability to obtain counsel's advice precisely when they needed it most (Office of the Inspector General).

According to the Military Commissions Act of 2006, the term "alien" means an individual who is not a citizen of the United States. The term "unlawful enemy combatant" means an individual determined by or under the authority of the President or the Secretary of Defense: a) "to be part of or affiliated with a force or organization; including but not limited to al Qaeda, the Taliban, any international terrorist organization, or associated forces—engaged in hostilities against the United States or its co-belligerents in violation of the law of war; b) to have committed a hostile act in aid of such a force or organization so engaged; or c) to have supported hostilities in aid of such a force or organization so engaged. "Alien unlawful enemy combatants, as defined in 16, section 948a of this title, shall be subject to trial by military commissions as set forth in this chapter (10). The United States was once considered to be a world leader for democracy and we need to utilize the existing, established law accordingly. Laws already exist for prisoners of war, spies, those committing espionage and domestic criminals. Creating new laws that, when examined by the Supreme Court, are unconstitutional, and/or circumvent existing laws, in an automatic response to fear, is not the answer. Perhaps trial by the International Court of Justice is the answer. It would certainly go a long way to reestablishing the United States as a world leader in human rights.

There is a clear delineation between prisoners of war (POW), enemy prisoners of war (EPW), and other detainees. Geneva Convention Relative to the Treatment of Prisoners of War (GPW) and the United States Army define the following: enemy prisoner of war (EPW) is a detained person, as defined in Articles 4 and 5 of the GPW, in particular, one who, while engaged in combat under orders of his or her government, is captured by the armed forces of the enemy. As such, he or she is entitled to the combatant's privilege of immunity from the municipal law of the capturing state for warlike acts that do not amount to breaches of the law of

armed conflict. For example, an EPW may be, but is not limited to, any person belonging to one of the following categories of personnel who have fallen into the power of the enemy: a member of the armed forces, organized militia or volunteer corps, a person who accompanies the armed forces without actually being a member thereof, a member of a merchant marine or civilian aircraft crew not qualifying for more favorable treatment, or individuals who, on the approach of the enemy, spontaneously take up arms to resist invading forces (Department of the Army). Other detainees are persons in the custody of the U.S. Armed Forces who have not been classified as an EPW (Article 4, GPW), retained personnel (Article 33, GPW), and civilian internees (Articles 27, 41, 48, and 78, GC) shall be treated as EPWs until a legal status is ascertained by competent authority, for example, by Article 5 Tribunal (Department of the Army).

Torture

As Americans we should not advocate torture as a means to extract information. From a legal standpoint the repercussions that would descend on America for conducting torture can be severe, as the soldiers who participated in the Abu Ghraib prisoner abuse scandal are now finding out. The simple answer, "I was following orders," does not hold in today's military (FOX News). The My Lai massacre in Vietnam was atrocious but it has had a sweeping effect upon how the military views and reacts to torture. Although many other countries use torture to extract information, if the US starts to extract information through torture, we are opening up the doors to our enemies who use it, that we now condone torture (Fox News).

I offer the following: torture is not as reliable as other methods (psychological) of gathering information. I am fully aware of the mental and physical aspects of torture and understand that terrorists do not abide by the same rules. If you beat an individual and ask

questions, he will provide answers and tell you what you want to hear. Is the information reliable? Is the source considered credible?

Political scientist Harold William Rood, who for ten years taught field interrogation of prisoners of war in military intelligence schools, explained the institutionalization challenge as follows: many agencies must coordinate in a counterterrorist operation. Reliability and accountability are therefore essential. Outlaws and madmen cannot be hired as torturers by an otherwise orderly agency. The torturers have to be well trained and professional: "To deliberately torture a person over a period of six weeks is asking a lot of human beings. And therefore you have to recruit them very carefully." This is the work of a highly trained team of interrogators (Arrigo, J).

Congress has introduced legislation to limit the rights of enemy combatants to challenge their detention in federal court while other measures, led by Senator McCain, seek to close loopholes in current anti-torture laws. Senator McCain served as a naval aviator seeing combat in the Vietnam War and was held as a prisoner of war for five and a half years, from 1967 to 1973. He understands torture and the implications of utilizing these methods. Furthermore, as Colin Powell and others have argued, if the United States unilaterally reinterprets Common Article 3 of the Geneva Conventions to permit torture, potential adversaries in future conflicts will feel justified in doing the same thing (Arrigo, J).

Preemption and Foreign Policy

When it comes to fighting terrorism the option of preemptive action is necessary in foreign policy because successful terrorism does not warn its victims of impending danger. It is by nature covert and depends on evading detection until the attack is complete. Defending against terrorism requires advanced knowledge of the identities of the terrorists and their

intentions whenever possible. Obtaining that information and neutralizing terrorists before they can strike involves preemptive thinking on our part. It is this mode of thinking that is part of the preemption debate. This policy is somewhat foreign to both the popular and legal thinking in the United States and abroad. But this is primarily because we and the international community are at ease using surveillance, detection, and apprehension methods to find, arrest, and try criminals who have committed crimes, but not those who have yet to commit them. For this reason and others, serious concerns about preemption abound as a legitimate foreign policy strategy (US Department of State).

But in meeting the threats we face, we need to think differently about the world we live in and the foreign policy decisions we make to defeat terrorism. For decades the United States has addressed these threats as a criminal problem. But according to some terrorism experts we need to go beyond the legal system and treat terrorism as a political issue, which can affect foreign policy. Such policies demand the collaborative efforts of the executive and legislative branches to provide an objective and measured response in the face of danger.

For example, the US PATRIOT Act enacted after 9/11 enabled the United States "to begin improved information sharing between the intelligence communities and law enforcement domestically and internationally. This resulted in the State Department designating 39 entities as terrorist organizations pursuant to the Patriot Act; 110 individuals were brought up on criminal charges, 60 of whom are in federal custody. The INS has detained 563 individuals on immigration violations alone…" (Ashcroft), all resulting from the collaborative efforts of the legislative and executive branches.

In cooperation through the UN many countries have signed international agreements to deal with terrorism. There are eighteen such agreements covering such topics as sending accused

terrorists to other countries to face trial and returning hijacked airplanes. Not all countries have signed these agreements, and some countries do not abide by their terms, so they are not always effective. Some of the detainees being held in Guantanamo Bay, Cuba have been questioned and interrogated and were due to be sent back to their homelands, who don't want them. The international conventions do not always work, and they are not always followed by countries that harbor, or provide a safe place, for terrorists. But they provide justification for countries that do sign the conventions to enforce the rules or to punish countries that do not. Such punishment can include seizing financial assets or banning international trade with such countries (United Nations-CT).

Immediately following September 11, the federal government started to use the immigration system as one of its primary tools in their investigation into the attacks on the World Trade Center and the Pentagon. Attorney General John Ashcroft made clear that he intended to use the immigration system's lax standards of protection to circumvent individual rights that are protected in our criminal justice system. On October 25, 2001 Ashcroft told a meeting of the United States Conference of Mayors that "taking suspected terrorists in violation of the law off the streets and keeping them locked up is our clear strategy to prevent terrorism within our borders" (Ashcroft, J). To Ashcroft this policy meant that "if you overstay your visa, even by one day, we will arrest you. If you violate a local law, you will be put in jail and kept in custody as long as possible" (Ashcroft, J). The government has chosen to assume that individuals with immigration violations, particularly Muslim, Middle Eastern, or South Asian men, are terrorists until proven otherwise (Ashcroft). American policies and actions have kept the homeland safe from attack for a decade. Over the course of the 10 years, American authorities foiled more than

two dozen al-Qaeda plots. U.S. authorities have managed to keep America safe from al-Qaeda for a decade; by the time he was killed, Osama bin Laden was barely a leader (Ashcroft, J).

There is debate about the use of military force to protect the human rights of individuals in other nations. This kind of debate stems largely from a tension between state sovereignty and the rights of individuals. Some defend the principles of state sovereignty and nonintervention and argue that other states must be permitted to determine their own course. It is thought that states have diverse conceptions of justice, and international coexistence depends on an ethic where each state can uphold its own conception of the good. States that presume to judge what counts as a violation of human rights in another nation interfere with that nation's right to self-determination.

In addition, requiring some country to respect human rights is liable to cause friction and can lead to far-reaching disagreements. Therefore, acts of intervention may disrupt interstate order and lead to further conflict. Past experience has demonstrated that the protection of human rights is not simply a matter of building consensus and will, but rather is intertwined on a larger scale with issues of development, freedom, and justice. In turn, development and justice depend inherently on sharing, at both the individual as well as the international level (Donnelly, J). The success of sharing resources to secure human rights has been demonstrated many times by a multitude of human rights programs and occasionally on a larger scale by programs such as the International Red Cross, the Marshall Plan, and various United Nations programs.

The threat posed by terrorists should not obscure the importance of human rights. How far should we go with this? Extra precautions have to be put in place to insure that the United States is doing everything possible to save and preserve human life against terrorist attacks in the future. Historically, the United States has been expansive in its compliance with the requirements

of international humanitarian law (the laws of war) with regard to belligerents captured in the course of an armed conflict. For example, the United States afforded prisoner-of-war status to Chinese soldiers captured during the Korean War even though the Peoples Republic of China was not a party to the 1949 Geneva Convention. It provided POW status to many captured guerrillas during the Vietnam War. During the 1991 Gulf War, the U.S. military convened special tribunals to determine the legal status of more than one thousand captured Iraqis, as the Geneva Convention required (Roth). The Bush administration broke with this long tradition in its treatment of terrorist suspects and others detained in the war against terrorism. The Bush administration also breached the rule of law to take custody of some detainees. In October 2001 it sought the surrender in Bosnia of six Algerian men who were suspected of planning attacks on Americans. After a three-month investigation, Bosnia Supreme Court ordered the men's release from custody for lack of evidence. When rumors spread of U.S. efforts to seize the suspects anyway, the Bosnia Human Rights Chamber, which was established under the US-sponsored Dayton Peace Accord and includes six local and eight international members, issued an injunction against their removal. Yet in January 2002 under U.S. pressure, the Bosnian government ignored this legal ruling and delivered the men to U.S. forces, who whisked them out of the country, reportedly to Guantanamo (Roth, K).

United Nations Universal Declarations of Human Rights

Though most countries have signed the United Nations Universal Declarations of Human Rights, many human rights issues remain unaddressed and unresolved. The enforcement of international humanitarian law is critical not only for the protection of civilians living under occupation, but also in preserving prospects for peace and security. Human rights are frequently held to be universal in the sense that all people have and should enjoy them. They are

independent in the sense that they exist and are available as standards of justification and criticism whether or not they are recognized and implemented by the legal system or officials of a country. Human rights rest upon moral universalism and the belief in the existence of a truly universal moral community comprising all human beings (United Nations).

Moral universalism posits the existence of rationally identifiable trans-cultural and trans-historical moral truths. There is much disagreement about when and to what extent outside countries can engage in human intervention. More specifically, there is debate about the use of military force to protect the human rights of individuals in other nations. This sort of debate stems largely from a tension between state sovereignty and the rights of individuals (Donnelly, J). Some defend the principles of state sovereignty and nonintervention and argue that other states must be permitted to determine their own course. It is thought that states have diverse conceptions of justice, and that international coexistence depends on an ethic where each state can uphold its own conception of the good. States that presume to judge what counts as a violation of human rights in another nation interfere with that nation's right to self-determination. In addition, requiring some country to respect human rights is liable to cause friction and can lead to far-reaching disagreements (Donnelly, J).

Therefore, acts of intervention may disrupt interstate order and lead to further conflict. Past experience has demonstrated that the protection of human rights is not simply a matter of building consensus and will, but is intertwined on a larger scale with issues of development, freedom, and justice. In turn, development and justice depend inherently on sharing, at both the individual as well as the international level. The success of sharing resources to secure human rights has been demonstrated many times by a multitude of human rights programs and

occasionally on a larger scale by programs such as the International Red Cross, the Marshall Plan, and various United Nations programs.

Conclusion

The United Nations Declaration of Human Rights is a thirty article declaration that lays out, explicitly, the fundamental rights inherent in mankind. Despite the important progress made in the discussion of collective rights in the last decades, a great deal remains to be done to resolve outstanding issues regarding those rights. To achieve a comprehensive understanding and united approach among governments and indigenous peoples on their rights will take a long time (United Nations).

I believe it is necessary to give up some civil liberties in order to make the country safe from terrorism. I don't believe that we have lost many, if any, of them. I made the comment that we Americans are spoiled and believe we are entitled to everything. It may become necessary to give up certain rights that we cherish those same rights that some people of the world have never even had the pleasure to enjoy. As wrong as it may seem, I don't think that terrorists should enjoy the freedoms of the rest of the free world.

The bottom line is that human beings, regardless of differences in circumstance, nationality, religion, physical condition, race, gender or age possess a basic and unconditional dignity that must be respected by governments and other people. Will there ever be true equality? Unfortunately I think the answer is no. The various and different cultures and mindsets around the world will affect total equality for all. The rest of the world looks at the United States for more than just aid or money. Because we are a world leader, others look to us for guidance. What they see are the strange turns that a great nation that holds its Constitution and laws sacred has taken.

The Universal Declaration of Human Rights provides a designed goal for humanity, but we are far from achieving universal implementation. The protection of human rights has complex issues and problems that span the entire range of human experience. The simple first step in reaching a workable and lasting solution is to implement the principle of sharing on as wide a scale as possible. Not only are there sound arguments and historical evidence to support this approach, but it also remains a fact that essentially everything else has already been tried.

References

Arrigo, J.M. (1999). A Consequentialist Argument against Torture Interrogation of Terrorists. Joint Services Conference on Professional Ethics January 30-31, 2003, Springfield, Virginia. Retrieved from http://www.au.af.mil/au/awc/ awcgate/jscope/arrigo03.htm

Amnesty International USA. Universal Declaration of Human Rights. Retrieved October 19, 2011 from http://www.amnestyusa.org/udhr.html 8.

Ashcroft John, Attorney General Prepared remarks for the US Mayors Conference, Oct. 25, 2001. Retrieved from http://www.usdoj.gov/ag/speeches /2001/ agcrisisremarks10_25.htm

Encyclopedia Britannica. Human Rights. Retrieved from http://www. britannica.com /eb/article-9106289/human-rights 1

Davis, Thomas Patriot Act at 10: Collective Safety v. Individual Freedom. Retrieved from http://open.salon.com/blog/tpd)

Department of the Army. (2006). FM 2-22.3 (FM 34-52) Human intelligence collector operations. Washington D.C.)

Donnelly, Jack, International Human Rights (3d ed.), Westview Press (2007)

Donnelly Jack, Universal Human Rights in Theory and Practice (2d ed.), Cornell University Press (2003)

FOX News May 21, 2004 Prison Abuse Soldiers: 'We Were Following Orders'. Retrieved October 20, 2011from http://www.foxnews.com/story/0,2933,120528,00.html

Georgetown (Session, 1. C. (2006, Oct 17). Military Commissions. Retrieved from

Georgetown Law. http://www.law.georgetown.edu/faculty /nkk/ documents /MilitaryCommissions.pdf)

High Commissioner for Human Rights. Retrieved from http://www.ohchr.org /english /about/structure.htm 9/10

Office of the Inspector General, U.S. Department of Justice, The September 11 Detainees: A Review of the Treatment of Aliens Held on Immigration Charges in Connection with the Investigation of the September 11 Attacks,. June 2003 Retrieved from http://www.usdoj.gov/oig/special/03-06/index.htm

Roth, Kenneth. Justice and the 'War' against Terrorism: Beyond the Law Retrieved from http://www.hrw.org/en/news/2003/01/05/justice-and-war- against-terrorism

The United States Constitution. U.S. House of Representatives. 28 Jan. 2005. Retrieved From http://www.archives.gov/exhibits/charters/constitution_transcript.html

United Nations. Universal Declaration of Human Rights. Retrieved from http://www.un.org/Overview/rights.html 7.

United Nations-CT. United Nations Global Counter-Terrorism. United Nations General Assembly Adopts Global Counter-Terrorism Strategy Retrieved from Strategyhttp://www.un.org/terrorism/strategy-counter-terrorism.shtml

USA PATRIOT Act." Electronic Privacy Information Center. Retrieved from http://www.epic.org/privacy/terrorism/usapatriot/

U.S. Department of State. Bureau of Democracy, Human Rights, and Labor. Retrieved from http://www.state.gov/g/drl/hr/ 4

U.S. Dept. of State. (2001). "Ashcroft Says terrorism Investigation Aims to Protect Lives." U.S. Dept. of State International Information Programs (IIP). Retrieved from

http://usinfo.state.gov/topical/pol/terror/01120610.htm

U.S. Department of State. Bureau of Democracy, Human Rights, and Labor. Retrieved from http://www.state.gov/g/drl/hr/ 5.

U.S. Government. The National Strategy for Homeland Security 2007.

White House. United Nations Headquarters, New York, New York. President Speaks to the United Nations General Assembly Retrieved from http:// www.whitehouse.gov/news/releases/2004/09/20040921-3.html 6.

Wikipedia. Human rights. Retrieved from http://en.wikipedia.org/wiki /Human_rights.

U.S. Government. Military Commissions Act of 2006 Retrieved from http://www.loc.gov/rr/frd/Military_Law/pdf/PL-109-366.pdf

Chapter 9

National Preparedness through Public, Private and Federal Partnerships

Multidisciplinary approaches to homeland security

"Homeland Security cannot begin and end at the doors of our federal department building in Washington, D.C. Washington can be expected to lead, but we cannot, nor should not, micro-manage the protection of our country. Instead, it must be a priority in every city, every neighborhood, and every home across America."

Secretary Tom Ridge

"May I stress the need for courageous, intelligent, and dedicated leadership… Leaders of sound integrity. Leaders not in love with publicity, but in love with justice. Leaders not in love with money, but in love with humanity. Leaders who can subject their particular egos to the greatness of the cause."

Dr. Martin Luther King, Jr.

There can be no question that emergency management has the moral and ethical responsibility to plan and provide for all citizens equally, to prepare for and respond to critical needs during and after an emergency or disaster, and to ensure that the vulnerable people in the surrounding communities are included in the process. Terrorism and natural disasters have occupied the minds and awareness of Americans in recent years. However, there are still unknowns about the thought process behind resilience and preparedness. Whatever improvements have been made to our capacity to respond to natural or man-made disasters ten

and half years after 9/11, we are still not fully prepared; there are many theories and perspectives that are often conflicting and confusing.

In an ideal world every individual, agency, and local jurisdiction would be fully prepared for all hazards and disasters. Unfortunately, research indicates that only 35% of the U.S. population reports having taken any preparedness measures (Citizen Corps). Instead, 37% of the populations expects first respondents (i.e., fire and police) to arrive on their doorsteps within one hour of a disaster onset; and a full 2/3 of the American population think help will arrive within a few hours (Redlener, I).

This comes at a time when the resources of local jurisdictions are shrinking, and many are struggling to meet routine operational costs. A major disaster will overwhelm local capabilities, and it may easily take three days or more for outside assistance to arrive. Adding to the difficulty, the proliferation of lawsuits tells local governments and emergency management professionals that current planning efforts are often inadequate when it comes to reaching beyond the mainstream populations. They argue that all planning and response activities must be fully "inclusive" and capable of dealing with all the potential needs for all populations, including those with physical or cognitive disabilities and other barriers. This requires additional, focused effort when personnel and resources are stretched thin already; and even emergency managers may not be entirely sure what is expected of them. The fact that public expectations may be unreasonable only adds to the challenge.

In 2003 President Bush directed the development and implementation of the National Incident Management System (NIMS) through the Homeland Security Presidential Directive 5 (HSPD-5). NIMS is designed to provide a common, consistent approach for emergency management officials to respond to and recover from hazards.

On August 23, 2005 Hurricane Katrina formed as a tropical storm off the coast of the Bahamas. Over the next seven days the tropical storm grew into a catastrophic hurricane that made landfall first in Florida and then along the Gulf Coast in Mississippi, Louisiana, and Alabama, leaving a trail of heartbreaking devastation and human suffering. Katrina wreaked staggering physical destruction along its path, flooded the historic city of New Orleans, ultimately killed over 1,300 people and became the most destructive natural disaster in American history. The fear of the sheer ferocity of nature was soon matched with disappointment and frustration at the seeming inability of local, state and federal governments to respond effectively to the crisis. Hurricane Katrina and the subsequent sustained flooding of New Orleans exposed significant flaws in preparedness for catastrophic events and our capacity to respond to them (Townsend, F).

Effectively organizing government structures for homeland security activities is still a work in progress. Following the deadly terrorist attack on September 11, 2001 and Hurricane Katrina in August and September of 2005, questions still generate with respect to the most effective organizational structure for federal and state governments in responding to natural and terrorist-related disasters. The potential consequences of not having answered these questions, however, are much easier to identify. The negative consequences of ineffective organizational structures include sporadic and unreliable information-sharing, fragmented preparedness and response strategies, inefficient use of scarce resources and, potentially and most importantly, the needless loss of lives and property.

No organization has the capability to deal singlehandedly with the preparation for, prevention of, response to, or recovery from a multi-jurisdictional natural or man-made disaster. Natural disasters such as hurricanes, wildfires and terrorist attacks do not recognize geographical

or jurisdictional boundaries, thus increasing challenges to both preparation and response. Coordination, collaboration, communication and cooperation are all necessary to achieve unity of effort in preparedness, prevention, response, and recovery. It is important to engage and educate the public and media on homeland security issues because they play very large roles in the response to a disaster. Educating them on predicted actions, and actions they can take to protect themselves, are keys to efficient and productive disaster responses (Gerencser, M).

The Preparedness Cycle

The preparedness cycle is comprised of seven essential phases; no matter the size of a sector or organization, all plans should follow the same construct. Mastery of these tasks will improve the ability of any community to address a full range of hazards. A key way to determine how prepared a county, region, or state should be are three questions: how prepared do we need to be, how prepared are we, and how do we prioritize efforts to close the gap.

DHS has provided a vast amount of material to assist communities at all levels. One of those tools is the Emergency Support Function (ESF), basically lists of capabilities in organizational structure to provide the support, resources, program implementation and services that are most likely to be needed to save lives, protect property and the environment, restore essential services and critical infrastructure and help victims and the community to return to normal (NRF).

Figure 1

Planning makes it possible to manage the entire life cycle of an emergency, determine capability requirements, and help stakeholders learn their roles and respond to an incident capably and efficiently. It includes the collection and analysis of intelligence and information, as well as the development of policies, procedures, plans, mutual aid/assistance agreements, strategies and other arrangements necessary to perform the EM mission. The planning process is dynamic and involves an ongoing system of updating plans based on results of drills, exercises, responses, changes in local, state, and federal rulings, updated knowledge about hazards and changes based on best practices of other jurisdictions (FEMA).

Organizing to execute response activities includes developing an overall organizational structure, strengthening leadership at all levels and assembling well-qualified individuals and teams for essential readiness, response, and recovery tasks. The National Incident Management System (NIMS) provides standard command and management structures which apply to incident response (FEMA).

Training to build essential readiness, response, and recovery capabilities requires a systematic program to meet a common baseline of performance standards (FEMA).

Equipping personnel with the necessary resources to perform assigned EM missions is an essential component of preparedness. Effective preparedness requires the identification, acquisition, deployment and sustainment strategies needed to conduct response and recovery missions; this includes the capability to communicate with the public, first responders/receivers and mutual aid partners, and higher headquarters (FEMA).

Exercises provide opportunities to assess plans and capabilities and improve proficiency in a risk-free environment. Exercises are also a valuable tool for assessing and improving performance while demonstrating community resolve to prepare for major incidents (FEMA).

Evaluating is a systematic assessment process that leads to judgments and decisions about plans, programs or policies (FEMA).

Taking Corrective Action ensures a continual process of EM program improvement. A functional corrective action program will provide a method and define roles and responsibilities for prioritization, assignment, monitoring and reporting of corrective actions arising from training, exercises and actual emergencies (FEMA).

Disciplines Associated with Needed Resources

It is impossible to plan properly for a disaster if it causes unexpected disruptions on an organization. Assessing the impact of an event includes not only estimating the quantitative or economic losses but also the collective impact on the organization's ability to operate, i.e. effects on personnel and the effect on the reputation of the organization. Homeland security is an ongoing and shared responsibility across the nation. There are numerous public and private sector stakeholders who influence the direction of homeland security; all must work together to

develop and implement the homeland security strategy by building and maintaining necessary capabilities (NRF).

FEMA has provided the emergency management community with some extremely useful tools, specifically lists of Mission Essential Functions (MEFs), which refers to those functions of such importance that they must be performed during, and in the immediate aftermath, of an emergency and which cannot be postponed longer than 24 hours. MEFs that cannot be executed may be transferred to another organization. There are a total of fifteen FEMA Emergency Support Functions (ESF) which provide the structure for coordinating federal interagency support for a federal response to an incident (FEMA).

The National Response Framework (NRF) details 15 ESFs in place to coordinate operations during federal involvement in an emergency: transportation, communications, public works, engineering, firefighting, information and planning, mass care, resource support, health and medical services, urban search and rescue, hazardous materials, food and energy. Emergency management provides the means for coordinating resources and assets necessary to alleviate the impact of an emergency or disaster on residents and public entities. Coordination occurs between emergency management entities and federal, state, county and local jurisdictions as well as with volunteer agencies and private business.

Differences between Emergency Management and Homeland Security

The U.S. Department of Homeland Security (DHS), a federal agency established in response to the terrorist attacks of September 11, 2001, has three primary responsibilities: to prevent terrorist attacks inside the United States; to reduce the nation's vulnerability to terrorist attacks and the damage caused by them; and to coordinate quick and effective recovery if terrorist attacks occur (History).

The Department of Homeland Security, according to its assigned response mission, is to lead, manage and coordinate the national response to acts of terrorism, natural disasters, or other emergencies. The challenge for public safety and security is that the federal government only provides assistance when local agencies are overwhelmed or are depleted. The fundamental responsibility of public safety falls with local and state governments. DHS coordinates its activities with other federal entities devoted to national security, particularly intelligence agencies, such as the Central Intelligence Agency (CIA), the U.S. military, and the Federal Bureau of Investigation (FBI). In addition DHS works with state and local agencies that provide the first government assistance following a terrorist attack (History).

The Federal Emergency Management Administration (FEMA) is an agency within DHS and the federal government that is responsible for emergency planning and preparedness, as well as recovery assistance and coordination following natural or human-caused disasters. Depending on the situation, FEMA either provides direct assistance to those in need or works with various federal, state, local, and nonprofit agencies to coordinate responses to emergency situations. The goal in response to disasters is to lead, manage and coordinate the national response, not the local response. This response is crucial to ensuring the health and welfare of the survivors of the disaster. They are responsible for reducing the loss of life and property and protecting the nation from all hazards. FEMA is divided into 10 regions; its job it is to work with the Emergency Managers from the states to procure the appropriate response from the federal government (FEMA 3).

Emergencies that warrant either a local, state, or federal effort can include a variety of situations. Natural disasters include earthquakes, floods, tornados, hurricanes, blizzards, mud-slides, and volcanoes; fires can be set accidentally (by lightning storms or by careless campers)

or they can be set deliberately by arsonists; transportation disasters include airline crashes, train crashes and derailments, boat accidents, highway pileups and accidents, and anything that disrupts the ability of people to move from one place to another; hazardous materials emergencies include oil spills, hazardous waste spills, and nuclear accidents; invasions and attacks could come from military or terrorist sources. Depending on the size and location of the emergency, local municipalities may take the primary charge, with state and federal agencies providing backup. Emergency management can also come from the private or corporate sector; mining accidents, for example, are usually handled primarily by the mining company whose on-site miners are most familiar with the safest and most efficient rescue procedures.

Civilian agencies can offer a great deal of aid during emergencies, in part because, thanks to large networks, they are able to mobilize supplies and volunteers quickly. Two of the oldest and best known are the American Red Cross and the Salvation Army. The private sector can play a vital role in emergency management, both during and after the emergency event. Businesses that have specialized skills, in transportation, for example, can provide trained volunteers and equipment to assist in emergency management efforts. A food services business can provide meals for emergency personnel. Companies with excess space can house equipment or people.

"State and local levels of governments have primary responsibility for funding, preparing, and operating the emergency services that would respond in the event of a terrorist attack."

National Strategy for Homeland Security, July 2002

Megacommunity and Whole Community Concepts

A megacommunity is a new approach to solving problems which cover business, government and the communities in which we live. A megacommunity is a region in which

multifaceted problems exist and are addressed in a collaborative environment. Here leaders interact according to their common interests, while maintaining their unique priorities; simply put it is a tool which can examine complex problems in new ways. The five critical elements of a megacommunity are tri-sector engagement, overlap in vital interests, convergence, structure and adaptability. "The objective for each organization operating in a megacommunity is achieved by optimizing its interests instead of maximizing; all participants gain. Best of all, operating in a megacommunity is not a zero-sum game" (Gerencser, M).

Multidisciplinary relationships are groups of teams or people from different disciplines who come together for a common purpose. The approach is used in a variety of settings including fires, natural disasters, sewage spills, HAZMAT issues, and terrorism. The concept is that it is best to address an issue or problem from all angles. For an emergency management setting this means a holistic approach focusing on a variety of mission essential functions (NRF). The multidisciplinary relationship is typically used in difficult and complicated situations where a comprehensive response has the best chance of accomplishing the goals. Emergencies and natural disasters come in many forms such as oil spills, earthquakes, tornados, floods, blizzards, fires, and volcanic eruptions. A particular disaster may be limited to one specific region, meaning that people in certain areas have only to prepare for those disasters which are likely to happen in their region.

I pose the common sense approach. First and foremost, there needs to be a good relationship between stakeholders: if the surrounding communities can't get along, then there won't be any partnerships created. If the leaders of the community get along, this helps create a non-hostile environment, and if the leaders support a program or process, their subordinates will do the same.

Once the community comes together a charter needs to be established. A vision and mission statement needs to be developed from the beginning. In my opinion the one in charge during the forming of the relationship depends on who has the most to provide and lose. Additionally resources shouldn't be just doled out arbitrarily. All stakeholders should provide their time, although sometimes this will be burdensome; they will need to be part of a team to help mitigate and respond to incidents that may occur in their jurisdiction. "Involvement in a megacommunity allows any participating [member] that is part of any sector to use the abilities, the understanding, and even the prejudices of the other sectors" (Gerencser, M).

According to the FEMA web site, "many states and big cities are actively entering into public-private partnerships to improve their capabilities in emergency management." Every jurisdiction is in a resource crunch and we will see, as resources dwindle more rapidly than expected, the relationships will only get stronger. FEMA also states: "We can share successful models and best practices" (FEMA 2). Many of the military branches currently utilize best practices web sites. More often than not, one organization's best practice can save thousands of dollars and man hours simply by sharing the information.

The Community and Regional Resilience Initiative is a very well thought out and prepared document. It does not answer all the questions everyone will have, but it is a great starting point for agencies that have nothing in place; the most important aspect of this document is that it encourages agencies, organizations, and communities to start thinking (CARRI). The majority of the documents on the FEMA site (FEMA 2) were prepared by non-profit organizations and for the most part outline what communities need to practice or do. A continuous flow of critical information needs to be maintained among multi-jurisdictional and multi-disciplinary emergency responders, command posts, agencies, and officials, for the

duration of the emergency response operation, in compliance with the NIMS. There needs to be structure and a process for ongoing collaboration between organization stakeholders at all levels; volunteers and nongovernmental resources need to be incorporated in plans and exercises; the public needs to be educated, trained, and aware; external partners need to be included in education, training, and exercise initiatives.

Multi-disciplinary Approaches to Homeland Security through Dialogue

There is no one-size-fits-all solution on how to plot a course for organizational change when the boss believes in holding to the status quo. But some idea of basic direction needs to be kept in mind when attempting to convince top management to support a multi jurisdictional partnership. To get an organization to communicate well internally, members must first want to be part of whatever the goal; they must take ownership or buy in. Once that occurs, the rest should come more easily.

According to DHS, metrics or benchmarks for achieving collaboration include "formalizing mutual aid agreements with surrounding communities and states to share equipment, personnel, and facilities during emergencies; conducting exercises of the execution of mutual aid agreements to identify the challenges and familiarize officials with resources that are available in the region; and coordinating homeland security preparedness assistance expenditures and planning efforts on a regional basis to avoid duplicative or inconsistent investments." Pre-planning at a regional level can also reduce stress during an actual event by the knowledge of available assets in a defined region, the knowledge and trust of those who will be responding to provide aid and assistance, and a defined set of roles and responsibilities according to National Incident Management System (NIMS) standards (FEMA 3).

The National Strategy for Homeland Security calls upon state governments to manage the

interface and inter-jurisdictional relationships of all the agencies, as well as the private sector, which have a role in homeland security. A major challenge is that, as in all other government programs, the expectations of all the stakeholders far outweigh any reasonable availability of resources. Additionally, there is no clear information or assessment concerning what metrics or characteristics would determine a successful state homeland security from one that is not.

Leveraging Existing Strengths in a Community

There is a need to encourage organizations providing community services to collaborate and work together instead of competing. It is recommended that the capacity of these organizations be promoted and strengthened, and that it include training in monitoring and evaluation. Coalitions of civil society organizations should be established to implement a coordinated response through a participatory and transparent process so that ordinary people can participate in a meaningful manner. Programs should ensure that the synergy and energy of community members as well as their experience and resources are enhanced. It is necessary to build on existing programs to provide the community a sense of ownership and to enhance their role in a community programs implementation (Gerencser, M).

How to Lead a Multi-disciplinary Approach to Homeland Security

Leaders must be able to interpret and focus on the big picture, plan and prioritize, improve performance influence, and manage resources. They must be able to lead and manage organizational environments that are responsive to change. They need to facilitate strategies to manage tensions between long-term program goals and the short-term organizational pressures. Leaders must be clever enough to apply leadership and management skills to effectively set a clear vision and guide entire community programs toward greater performance. The ability to formulate short and long-term goals for the megacommunity by selecting effective objectives

and determining priorities consistent with local goals is important; Anticipating and implementing innovative strategies to link strategic vision to core program capabilities are just a few requirements to lead in a multi-jurisdictional environment (Gerencser, M).

Federal Initiatives

The National Response Framework (NRF) is a 2008 iteration of the National Response Plan (NRP) which addressed the limitations contained within that document, the least not being the fact that the name itself was misleading as that document did not satisfy the requirements of a plan (NRF). The NRF recognizes that all disasters are different, and the conditions and resources available to respond will be different across communities. Essentially, the NRF can be adapted to any size and type event in any environment. The Framework commits the federal government to work as a partner with all governmental jurisdictions and the private sector, to develop appropriate response strategies, to address the broad range of emergency types for a range of emergency incidents outlined in the National Preparedness Guidelines. The NRF consists of several core documents which include the Emergency Support Function (ESF), support, incident annexes, and the Partner Guides. The main documents essentially provide national guidelines for response to all type emergencies by outlining the roles and responsibilities of responders, identifying responsible organizations, and listing other requirements to realize an effective and coordinated nationwide response to any emergency situation or event (NRF).

The ideals of the NRF are contained in five principles which constitute the "national response doctrine" (NRF). The national response doctrine outlines the roles, responsibilities and operational concepts of responders across all the relevant response agencies, NGOs and jurisdictions. Fundamentally, the objectives of all response activities are centered upon saving

lives, relieving human sufferings, quickly restarting economic activity and returning the natural and built environment to its pre-impact state. The key principles constituting the national response doctrine are: engaged partnership, tiered response, scalable, flexible, and adaptable operational capabilities, unity of effort through unified command, and readiness to act (NRF).

The Incident Command System (ICS) is a hierarchal command and control model designed to manage major events that involve a multijurisdictional and coordinated response among functional agencies, both public and private. It has a modular structure which allows for deployment and upgrade in an increasing complex situation and the integration of facilities, equipment and communications within an established command and control framework. The adoptability and flexibility in the ICS has facilitated its employment for varied events across diverse organizations. The utility of the ICS is that it not only provides a structure for command and control but also facilitates planning and other post event activities.

National Incident Management System (NIMS) is a system mandated by HSPD-5 that provides a consistent, nationwide approach for federal, state, local, and tribal governments, the private sector and non-governmental agencies to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity. To provide for interoperability and compatibility among federal, state, local, and tribal capabilities, the NIMS includes a core set of concepts, principles, and terminology. HSPD-5 identifies these as the Incident Command System, multi-agency coordination systems, training, identification and management of resources (including systems for classifying types of resources), qualification and certification, and the collection, tracking, and reporting of incident information and incident resources (NIMS).

Presidential Policy Directive (PPD) 8 was developed in the wake of several natural and anthropogenic events (such as the 9/11 terrorist attack, hurricanes Katrina and Rita, BP Deepwater Horizon Oil Spill and H1N1 influenza) which caused significant environmental, physical and physiological damage to the United States, and which stand as threats to the future safety and security of its citizens. Several approaches were taken to strengthen the resilience of the U.S. through what was described as "systematic preparation for the threats that pose the greatest risk to the security of the nation, including acts of terrorism, cyber-attacks, pandemics, and natural disasters" (PPD 8).

In addition to the four capability-specific national priorities listed throughout this project, the U.S. Department of Homeland Security has issued three overarching priorities and one additional capability-specific priority, for a total of eight national priorities. These priorities are:

1. Overarching priorities to implement the National Incident Management System and National Response Plan; expand regional collaboration; implement the National Infrastructure Protection Plan.
2. Capability-Specific priorities to strengthen information-sharing and collaboration capabilities; strengthen interoperable communications capabilities; strengthen CBRNE detection, response and decontamination capabilities; strengthen medical surge and mass prophylaxis capabilities; strengthen emergency operations planning and citizen protection capabilities

The national priorities are outlined in detail in the National Preparedness Goal, which was established under the direction of Homeland Security Presidential Directive 8 (HSPD-8). The vision of the goal is:

"To engage Federal, State, local, and tribal entities, their private and non-governmental partners, and the general public to achieve and sustain risk-based target levels of capability to prevent, protect against, respond to, and recover from major events in order to minimize the impact on lives, property, and the economy". (DHS)

The goal is designed in conjunction with other federal initiatives, including the National Planning Scenarios, the Universal Task List, and the Target Capabilities List. These initiatives are designed to provide capabilities-based planning tools to the states, locals, and tribal entities. The results are intended to provide a common approach to national incident management (FEMA 3).

Where Do We Want to Go

Presidents Bush and Obama have issued HSPD-5, HSPD-8, PPD-8, the NRF, and NIMS, among other directives and guidelines in order to effect necessary changes to the nation's readiness. The ultimate goal according to the collective documents appears to be to maximize collaboration amongst all levels of government and across as many jurisdictional lines as reasonably possible. Municipalities are to attempt to sustain their capabilities to manage disasters and engage all means at their disposal to include the private sector. Businesses often have unique processes and procedures as well as items that could be of great value to response agencies and government officials. Organizations such as Wal-Mart operate on a global scale and have thousands of single stores that make over a million dollars in sales per day in some cases. Therefore, they are well qualified to provide logistical support to a disaster operation.

A serious attempt has been made to integrate civilians into the national system for emergency management known as the National Incident Management System (NIMS) through volunteerism. There are teams across America in local communities called Community

Emergency Response Teams (CERT) (FEMA 3). A CERT program "educates people about disaster preparedness for hazards that may impact their area and trains them in basic disaster response skills, such as fire safety, light search and rescue, team organization, and disaster medical operations" (Citizens Corps). Utilizing the knowledge and skills attained in the classroom and exercises, CERT members may assist their neighbors and fellow employees following an incident until the arrival of emergency professionals. CERT members also are encouraged to take a more active role in emergency preparedness projects in their community.

Private sector partnerships, volunteer recruitment, and CERT training are all effective strategies being undertaken, yet there is currently little more than passive involvement of individuals through other networks. Most of the education is through internet websites which citizens must search to find. Unlike the days of civil defense, organizations are not being leveraged to handle the immediate needs of communities and neighborhoods to sustain them for the first 72 hours after a disaster strike. It is during this time that the stage is set for success or failure; this can be greatly impacted by civilians on the ground as seen in past disaster cases.

Disaster response within the United States has an established and structured system which if properly utilized can significantly reduce the impact of natural and manmade events on the natural and built environment. Within this frame work is the National Incident Management System (NIMS) which is a template to enable multi-jurisdictional and multi-sector cooperation to prepare, prevent, respond, recover from and mitigate the effects of all hazards regardless of cause, size, location, or complexity. This is achieved through the command and control structures within the Incident Command System (ICS) which integrates operational systems in a common organizational structure and facilitates multi-sector and multi-jurisdictional disaster response.

References

A Framework and Toolkit to Work Towards Whole-of-Community Engagement. Retrieved from http://www.engagingcommunities2005.org/abstracts/Aslin-Heather-final2.pdf

Center for Whole Communities (2006) A Brief Orientation to Dialogue. Retrieved from http://www.measuresofhealth.net/pdf/brief_orientation_dialogue.pdf

Chandra, Anita, et al., Building Community Resilience to Disasters: A Way Forward to Enhance National Health Security. Retrieved from http://www.rand.org/pubs/technical_reports/TR915.html

Community and Regional Resilience Institute (CARRI). Resilient Communities Are the Foundation of a Resilient America Retried from http://www.resilientus.org/

Citizen Corps Retrieved from http://www.citizencorps.gov/about/

(NIMS). Department of Homeland Security (DHS). (2008). National Incident Management System. Retrieved from: http://www.fema.gov/emergency/nims/

(FEMA) Department of Homeland Security (DHS). (Jan 2008) National Response Framework (NRF) Retrieved from http://www.fema.gov/pdf/emergency/nrf/nrf- core.pdf

(FEMA 2) Department of Homeland Security (DHS) Public Private Partnership Models Retrieved from http://www.fema.gov/privatesector/ppp_models.shtm

(FEMA 3) Federal Emergency Management Agency. About FEMA. Retrieved from http://www.fema.gov/

Disaster Preparedness. Retrieved from http://www.ncdp.mailman .columbia . edu/files/NCDP07.pdf.

FIGURE 1 Retrieved from http://www.bing.com/images/search?q= PREPAREDNESS +CYCLE&id=47AD5610C0BC0941292187DB58F0834236D7A0E9&FORM=IQFRBA

Gerencser, Mark, et al., Megacommunities: How Leaders of Government, Business and Non-Profits Can Tackle Today's Global Challenges Together, New York: Palgrave Macmillan 2008.

(History) Department of Homeland Security (DHS). Brief Documentary History of the Department of Homeland Security 2001 – 2008 retrieved from http://www.dhs.gov/xlibrary/assets/brief_documentary_history_of_dhs_2001_2008.pdf

Homeland Security Presidential Directive 5 (HSPD–5), (February 28, 2003) Retrieved from http://www.dhs.gov/xnews/releases/press_release_0105.shtm

Homeland Security Presidential Directive 8 (HSPD–8), (March 30, 2011) Retrieved from http://www.dhs.gov/xabout/laws/gc_1215444247124.shtm

(NRF) Department of Homeland Security**,** National Response Framework Retrieved from http://www.fema.gov/emergency/nrf/

Redlener, I., Abramson, D., Stehling-Ariza, T., Grant, R., & Johnson, D. (2007). The American Preparedness Project: Where the US Public Stands in 2007 on Terrorism, Security, and

The Infrastructure Security Partnership. A Whole Community Approach to Emergency Management. Retrieved from http://www.tisp.org/index.cfm?cdid=12046&pid=10260

Townsend, F. (2006). The federal response to Hurricane Katrina lessons learned. Washington DC: The White House. Retrieved from http://library.stmarytx.edu/acadlib/edocs/katrinawh.pdf

Chapter 10

Cyber Threats to Critical Infrastructure

Technology and Critical Infrastructure Protection

"Cyber terrorism could also become more attractive as the real and virtual worlds become more closely coupled, with automobiles, appliances, and other devices attached to the Internet."

Dorothy Denning

Prepared by Matthew J. Cassidy, Installation Antiterrorism Officer, United States Military Academy West Point, New York. The purpose is to identify the current assessment of potential threats (Cyber threats) against the U.S. Military Academy, its personnel and the Academy's potential vulnerability to those threats.

The purpose of this Masters Project is to analyze the national security threats that the United States, Department of Defense, Department of the Army and more specifically the United States Military Academy at West Point, must face with cyber-attacks from individual actors and enemy nations. Cyber-attacks are a severe threat to US national security that must not be underestimated. Cyber-attacks can not only threaten information security but could also cause physical harm to the country. The reason this sector is important to homeland security is the DoD is connected via various communication nodes. At West Point there is a non-secure internet Protocol Router Network (*NIPRNet) and* Secret Internet Protocol Router Network (*SIPRNet*). In addition to these two systems there is the worldwide web and numerous other web based sites.

The cyber sector was chosen for this Masters project in partial fulfillment of the requirements for Technology and Critical Infrastructure Protection course, but more importantly it is to provide valuable information to the senior leaders of the Military Academy in anticipation that some countermeasures or mitigation techniques will be used to combat cyber terrorism.

There are ways that the Military Academy can combat this growing threat. With a proactive approach and better coordination between various parts of the DoD, the threat of cyber-attacks can be met and the impact minimized. As Presidential Decision Directive 63 states, critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. West Point is a very different military facility; the installation has a combination of federal and civilian assets. Critical infrastructure includes telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private (PDD-63). Cyber-attacks vary in methods, severity and impact and have been used against many parts of the US infrastructure, including commercial and military targets. The source of these attacks is both domestic and foreign, and it is often difficult to discern the motives or the perpetrators of these attacks (FBI).

West Point is susceptible to many natural and terrorism (human-caused) hazards. Knowledge of these hazards, the installation's vulnerability to them, and the capabilities in place to prevent them allows community stakeholders (e.g., leaders, emergency planners and responders, employees and residents) to better assess and mitigate their risks, and to manage their consequences (NIPP). From an extended power outage to a terrorist incident, the potential for disruption of operations to the loss of life or damage to property is unprecedented. These dangers pose significant challenges for those involved in emergency planning, response and recovery operations because of resource limitations that may constrain the availability of emergency management personnel, equipment, and training (Lewis, T).

Survey of the Infrastructure Sector's Threats

There have already been numerous cyber-attacks against the U.S. government, U.S. interests and US allies. While attacks are often harmless, some have been successful in gaining access to

classified information or disrupting services. Many of these attacks are believed to have originated in China (Fox). West Point is susceptible to many natural and human-caused hazards. Knowledge of these hazards, their frequency, the installation's vulnerability to them, and the capabilities in place to stop them allows community stakeholders (e.g., leaders, emergency planners and responders, employees and residents) to better assess and mitigate their risks, and to manage their consequences (NIPP). The risk assessment is a crucial step and the basis for developing a multiyear strategic plan that defines the mission, goals, objectives and milestones for the West Point (Lewis, T).

West Point has experienced significant impacts from natural hazards including floods, storms, and wildfires. Beyond natural hazards, there are technological or human-caused hazards such as power failures, hazardous material (HazMat) spills, civil disturbances (i.e. protests, unauthorized demonstrations), and, terrorism (as well as cyber-terrorism) that may also pose a threat. Each of these dangers requires a risk assessment in order to understand and to mitigate against its impact potential. West Point can never be completely safe; total security is an unachievable goal. Therefore, the issue becomes what is an acceptable level of risk to guide installation strategies and investments? A key outcome of this process is defining an acceptable level of risk given this reality (Lewis, T). West Point, due to its location and mission, is vulnerable to the damaging effects of significant, and potentially devastating natural and human-caused hazards. Events may occur at any time and may create varying degrees of harm and hardship to individuals and damage to the installation facilities (Lewis, T).

For each vulnerability assessed, a hazard risk profile of high, moderately high, moderately low, and low was constructed utilizing the following criteria: scope or how widespread the hazard may be; cascade effects or the likelihood that secondary hazards may be

generated; frequency or historical rate of occurrence; hazard duration and recovery time; speed of onset or the potential warning time available, and impact or the consequences the hazard may have on West Point. Although there is no single, universally accepted definition of terrorism, the US Justice Department defines it as the use of force or violence against persons or property violating the criminal laws of the United States for purposes of intimidation, coercion, or ransom. Terrorists often use threats to create fear among the public, to convince citizens that their government is powerless to prevent terrorism and to get publicity for their causes (FBI). The Federal Bureau of Investigation (FBI) categorizes terrorism in the United States as one of two types—domestic terrorism or international terrorism. Domestic terrorism involves groups or individuals whose terrorist activities are directed at elements of our government or population without foreign direction. International terrorism involves groups or individuals whose terrorist activities are foreign-based and/or directed by countries or groups outside the United States, or whose activities transcend national boundaries (FBI). A terrorist attack can take several forms, depending on the technological means available to the terrorist, the nature of the political issue motivating the attack, and the points of weakness of the terrorist's target. Based on the risk assessments contained here, the following hazards were viewed as significant for West Point: Moderately High Hazards.

Terrorism, since 9/11, has been viewed as a significant threat to the United States. Terrorists continue to aggressively recruit, train, and plan against high-value US targets with the aim of producing mass casualties, visually dramatic destruction, and fear. Given its symbolism, West Point represents a high-value target for extremist groups and individuals.

Cyber threats or cyber attacks on West Point's infrastructure or communications systems pose a rapidly growing but little understood threat to installation security and could become a

decisive weapon of choice for those seeking to do harm. Information infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers, are increasingly being targeted for exploitation and potentially for disruption or destruction, by a growing array of adversaries (NIPP).

Moderately Low Hazard

Spring and summer storms, a common hazard in the Hudson Valley, usually characterized by strong winds, are frequently combined with heavy rain and dangerous lightning. Excluding winter weather events, this category of storms includes thunderstorms, hailstorms, hurricanes, and tornados (NWS).

Winter storms can range from a moderate snow over a few hours to a blizzard with blinding, wind-driven snow that lasts for several days. Many winter storms are accompanied by dangerously low temperatures and sometimes by strong winds, icing, sleet, and freezing rain (NWS).

Low Hazard

Power outages represent the most likely yet least dangerous hazard to affect West Point. Backup power sources and restoration history suggest high system reliability and low vulnerability to a widespread power failure.

	PROBAILITY			CONSEQUENCES			WARNING			RISK
	HIGH	MED	LOW	MAJOR	MODERATE	MINOR	MINIMAL	MODERATE	ADEQUATE	VALUE
Score	*3*	*2*	*1*	*3*	*2*	*1*	*3*	*2*	*1*	
NATURAL										
Severe Storm	*3*					*1*			*1*	*5*
Power Outage		*2*				*1*		*2*		*5*
HUMAN-CAUSED										
Power Outage		*2*				*1*		*2*		*5*
Cyber-Threat	*3*			*3*				*2*		*8*
Insider-Threat		*2*		*3*			*3*			*8*
Terrorism (General)			*1*	*3*			*3*			*7*

History of the Hazard (Terrorism).

Although there have not been acts of terrorism at West Point, the potential for this type of incident is present. West Point, as a symbol of America's ideals and military might, is vulnerable to terrorist acts from global and local groups and individuals. There is concern that radical groups associated with the environment, animal rights, anti-war or anti-US causes could create problems at West Point, although they are not present in any number or groups of significant size and there have been no overt threats to date.

Vulnerability Analysis.

The type of terrorist act determines vulnerability. Depending upon the individual or group cause, almost any facility, activity or person(s) on the installation could be a potential target for terrorist activity. Likely targets at West Point may be senior military leaders, high profile guests or event venues, cadets, and elements of the installation infrastructure (e.g. buildings and utilities). Critical facilities and special events may become more appealing during visits by high profile personalities and dignitaries. Sporting events such as football games and graduation may increase the probability of terrorist targeting. Additionally, high-level meetings and conferences provide terrorists an excellent environment in which to articulate their cause through violence. Terrorism comes in many forms including explosive detonation, chemical,

biological or radiological release, nuclear detonation, hijacking/kidnappings, arson, shootings and computer-generated attacks. One of the special considerations in dealing with the terrorist threat is that it is difficult to predict. One must know the minds and capabilities of various terrorists and terrorist groups. These are characteristics that terrorist organizations strive to conceal. Because all terrorists are not the same, the calculation is even more difficult.

West Point should use the existing processes and methodologies developed for the successful management of other hazards. Usually the plans and systems developed for other problems can serve as templates for developing a comprehensive counter-terrorism program. Any mitigation strategy should focus on creating an infrastructure that is difficult to attack, resilient to the consequences of an attack, and protective of its occupants should an incident occur. Examples of mitigation measures include providing community outreach and education to departments and individuals concerning actions they can take in preparation for possible terrorist events, disseminating real-time information on alert levels from the Homeland Security Advisory System, making individuals, families, and installations aware of steps they should be taking at each alert level, providing guidance on personal protective measures and what to do in situations involving chemical agents, biological agents, explosives, and radiological agents, providing information to installation activities on techniques to "harden" their facilities against possible attack.

These actions can help ensure that West Point personnel are aware of the simple steps they can take to be better prepared for the potential consequences of any terrorist attack and to anticipate and prevent such attacks. The goal is to help individuals learn how to make preparedness a part of their daily lives and improve their work and living places in the process. First responders must remember they are targets and that proactive steps need to be taken to

protect the crime scene and the evidence. Just like preparedness issues with all potential sources of disaster, public education is needed to help the citizens of our county recognize the threat.

This Masters project will focus specifically on cyber terrorism and threats. Cyber–terrorism is "the premeditated politically motivated attack against information, computer systems, computer programs, and data which results in violence against noncombatant targets by sub-national groups or clandestine agents." Terrorist groups are using computers and the internet to further goals associated with spreading terrorism, although the proportion of cybercrime that can be directly or indirectly attributed to terrorists is difficult to determine.

Hazard Identification: Cyber Threat

Just as the U.S. has capitalized on the use of computer technology, our adversaries have not overlooked the fact that they must also operate in the computer age. The sophisticated threat to our Global Information Grid, of which DoD and West Point are a part, is extensive and presents a real danger to national security. This threat includes nation-states that have openly declared their intent to develop cyber warfare capabilities. Further, it includes transnational and domestic criminal organizations, hacker groups, and terrorist organizations. The effects of a cyber attack align generally into four areas:

Loss of Integrity. System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality (AR-25-2).

Loss of Availability. If a mission-critical IT system is attacked and rendered unavailable

to its end users, the organization's mission will most likely be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users' performance of their functions in supporting the organization's mission (AR-25-2).

Loss of Confidentiality. System and data confidentiality refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from the jeopardizing of national security to the disclosure of Privacy Act data (AR-25-2).

Physical Destruction. Physical destruction refers to the ability to create actual physical harm or destruction through the use of IT systems. Much of our critical infrastructure, such as power and water, is operated with computer-controlled devices known as supervisory control and data acquisition (SCADA) systems. These systems can be attacked and used to cause operations to malfunction, such as the release of water from a dam or waste water facility or the disruption of the electrical power supply to the hospital. Any operation (e.g., academic records, supply records, office computer files) that make extensive use of computers are vulnerable to physical destruction through a cyber attack (NIPP).

History of the Hazard

Cyber-attacks vary in methods, severity and impact and have been used against many parts of the U.S. infrastructure, including commercial and military targets. The source of these attacks is both domestic and foreign, and it is often difficult to discern the motives or the perpetrators of these attacks (NIPP).

The U.S. Department of Defense has reportedly suffered an explosion in the number of cyber attacks conducted against its infrastructure since 2008. The number of cyber attacks

against the DoD has substantially increased over the past few years and a majority of them have originated from China (Harris). West Point has and will continue to be a target for cyber criminals due to its national profile and military background. DoD and DA computer networks are constantly being targeted by domestic and international organizations. The NEC West Point and the Army recognize the threat posed by cyber criminals and have implemented appropriate technical and procedural countermeasures aimed at detecting, preventing, reporting and responding to attempted network intrusions.

In November 2008 the Department of Defense (DoD), the Pentagon, and U.S. Central Command's (CENTCOM) computer networks were attacked. The cyber attack strike on those key facilities was/is thought to be from inside Russia. The DoD has traced the origins of the cyber-attack to an unauthorized flash drive that was inserted into a military laptop somewhere in the Middle East. A malicious code which was placed on the flash drive by an unspecified foreign intelligence agency uploaded onto a network run by CENTCOM. One report indicated that last year there were 71,000 incidents, and during the first half of this year 30,000 occurred. Not all incidents were able to penetrate the system. Although still high, approximately 2000 infiltrations occurred during this same time and some information was compromised (Lynn).

Vulnerability Analysis

This section lists vulnerabilities that may be found in typical IT systems. The order of these vulnerabilities does not necessarily reflect any priority in terms of likelihood of occurrence or severity of impact. Risk is a function of the likelihood (probability) that a defined threat agent (adversary) can exploit a specific vulnerability and create an impact (consequence). The risk induced by any given vulnerability is influenced by a number of related indicators, including:

Policy and Procedure Vulnerabilities.

Vulnerabilities are often introduced into IT systems because of incomplete, inappropriate, or nonexistent security documentation, including policy and procedures. Security documentation, along with management support, is the cornerstone of any security program. Installation IT security policy can reduce vulnerabilities by mandating conduct such as password usage, CAT-card protection, and internet usage. The following table describes potential policy and procedure vulnerabilities for IT systems.

Policy and Procedure Vulnerabilities	**Description**
Inadequate security policy	Vulnerabilities are often introduced into the system due to inadequate policies or the lack of policies specifically for system security
No formal IT security training and awareness program	A documented formal security training and awareness program is designed to keep staff up to date on organizational security policies and procedures as well as cyber security standards and best practices. Without training on specific policies and procedures, staff cannot be expected to maintain a secure communications environment
Inadequate security architecture and design	IT engineers have historically had no training in security and until relatively recently vendors have not included security features in their products
Absent or deficient IT equipment implementation guidelines	Equipment implementation guidelines should be kept up to date and readily available. These are an integral part of security procedures in the event of a system malfunction

Lack of administrative mechanisms for security enforcement	Staff should be held accountable for administering documented security policies and procedures
Few or no system security audits	Independent security audits should review and examine system records and activities to determine the adequacy of system controls and ensure compliance with established security policy and procedures. Audits should also be used to detect breaches in security services and recommend changes as countermeasures, which may include making existing security controls more robust and/or adding new security controls
No IT specific continuity of operations (COOP) or disaster recovery plan (DRP)	A COOP or DRP is needed in the event of a major hardware or software failure or destruction of facilities. Lack of a plan could lead to extended downtimes.
Lack of configuration change management	A process for controlling modifications to hardware, firmware, software, and documentation should be implemented to ensure the system is protected against inadequate or improper modifications before, during, and after system implementation. A lack of configuration change management procedures can lead to security oversights, exposures, and risks

Table 1 IT Policy and Procedures Vulnerabilities

Because every organization has a limited set of resources, organizations should perform a risk assessment for the IT systems and use its results to prioritize system components based on the potential impact to each system. The organization should then perform a detailed

vulnerability assessment for the highest-priority systems and assessments for lower-priority systems as deemed prudent/as resources allow (Lewis, T). The vulnerability assessment will help identify any weaknesses that may be present in the systems that could allow the confidentiality, integrity, or availability of systems and data to be adversely affected, along with the related cyber security risks and mitigation approaches to reduce the risks.

Platform Capabilities

IT system vulnerabilities can occur due to flaws, mis-configurations, or poor maintenance of platforms, including hardware, operating systems, and applications. These vulnerabilities can be mitigated through various security controls, such as OS and application patching, physical access control, and security software (e.g., antivirus software). Several platform vulnerabilities are depicted in the table below. The table below lists possible threats to West Point's information technology (IT) architecture. This list is in alphabetical order and not by greatest threat.

	Adversarial Threats to Information Technology Systems
Attackers	Attackers break into networks for the thrill of the challenge or for bragging rights in the attacker community. While remote cracking once required a fair amount of skill or computer knowledge, attackers can now download attack scripts and protocols from the internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use. Many attackers do not have the requisite expertise to threaten difficult targets such as critical U.S. networks. Nevertheless, the worldwide population of attackers poses a relatively high threat of an isolated

	or brief disruption causing serious damage
Bot-network operators	Bot-network operators are attackers; however, instead of breaking into systems for the challenge or bragging rights, they take over multiple systems to coordinate attacks and to distribute phishing schemes, spam, and malware
Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organized crime groups are using spam, phishing, and spyware/malware to commit identity theft and online fraud. International corporate spies and organized crime organizations also pose a threat to the US through their ability to conduct industrial espionage and large-scale monetary theft
Foreign intelligence services	Foreign intelligence services use cyber tools as part of their information gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare capabilities
Phishers	Spammers are individuals or organizations that distribute unsolicited e-mail with hidden or false information to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations
Spammers	Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware

Table 2. Adversarial Threats to IT Systems.

Network vulnerabilities can be eliminated or mitigated through various security controls, such as defense-in-depth network design, encrypting network communications, restricting network traffic flows, and providing physical access control for network components.

Mitigation Measures

West Point IT administrators should conduct and analyze the results of a comprehensive risk assessment, identify the cost of mitigation for each risk, compare the cost with the risk of occurrence, and select those mitigation controls where cost is less than the potential risk. Because it is usually impractical or impossible to eliminate all risks, the focus should be on mitigating risk with the greatest potential impact to the system. Additional mitigation measures include:

a) Developing a Comprehensive Security Program**.** Effectively integrating security into an IT system requires defining and executing a comprehensive program that addresses all aspects of security, ranging from identifying objectives to day-to-day operation and ongoing auditing for compliance and improvement.
b) Senior Leadership Buy-in**.** It is critical for the success of the IT security program that senior leaders buy into and participate in the IT security program.
c) Provide Training and Raise Security Awareness**.** Security awareness is a critical part of IT incident prevention. All organizations with access to the network should design effective training programs and communication vehicles to help personnel understand why control methods are required, ideas they can use to reduce risks, and the impact on the organization if control methods are not incorporated. Training programs also demonstrate leader's commitment to, and the value of, a cyber security program. Feedback from staff exposed to this type of training can be a valuable source of input for refining the charter and scope of the security program.
d) Define Specific IT Policies and Procedures**.** Policies and procedures are at the root of every successful IT security program. The more transparent these policies are with all

other procedures, the more likely they will be implemented at all levels. Policies and procedures help to ensure that security protection is both consistent and current to protect against evolving threats and also help to educate. After the risks for the various systems are clearly understood, the cyber security team should examine existing security policies to see if they adequately address the risks. Few organizations have the resources to harden the IT infrastructure against all possible threats; management should guide the development of the security policies that will set the security priorities and goals for the organization so that the risks posed by the threats are mitigated sufficiently. Security procedures should be documented, tested, and updated periodically in response to policy and technology changes.

Budget Proposal

Optimal Risk Reduction - Funding is allocated to reduce the mathematical risk - reducing vulnerability (probability of a fault) and risk (financial damages) (Lewis, T). Cyber crimes are costly and can do serious harm to an organization's bottom line; I have found during research that the median annualized cost of risk reduction is $3.8 million per year, but can range from $1 million to $52 million per year per company. Therefore the funding I am requesting will focus primarily on the external threat and the defense against cyber attacks. In order to properly protect the Information Technology sector at West Point the following budget would be submitted:

McAfee Total Protection for Secure Business $685,300.00. This program protects endpoints, encrypts data, scan and secure email, block spam, viruses, phishing attacks, and inappropriate content from entering your network. It has multiple layers of technology include IP reputation, domain name reputation, sender authentication, and grey listing; it has three layers of

protection include URL filtering, which can monitor and control web usage and enforce acceptable use policies; active malware scanning, which blocks malware trying to enter a network via the web (MacAfee).

One (01) Supervisory Information Technology Specialist (INFOSEC) GS -12 - $77,585. This position is to ensure the confidentiality, integrity, and availability of systems, networks, and data through the planning, analysis, development, implementation, maintenance, and enhancement of information systems security programs, policies, procedures, and tools. It will maintain the stability and currency of security software as applications and software change during the normal course of business, identify and evaluate future and emerging technologies in information security, disseminate information about the latest technology developments available in the marketplace through such activities as the preparation of briefings, various paper formats, and the arrangement of vendor presentations (CPOL).

Two (02) - Information Technology (IT) Specialists (INFOSEC) GS-11 $64,729 x2 = $129,458.00. These personnel provide advice and guidance in implementing IT security policies and procedures in the development and operation of network systems; they conduct risk and vulnerability assessments of planned and installed systems to identify vulnerabilities, risks, and protection needs, conduct system security evaluations, audits, and reviews, develop and implement training on system security policies and procedures for users and establish and maintain a comprehensive quality assurance program to cover file back and recovery, equipment maintenance, and quality control of systems processing and outputs (CPOL).

One (01) - Engineering Technician (Electrical)GS-09/11- $53,500 This individual is responsible for troubleshooting, maintenance, and repair on all makes of generators, and

diagnoses, repairs, adjusts, and modifies all components of the generator, engine and switch gear (CPOL).

Embed Information Technology/Information Assurance (IT/IA) concepts throughout West Point by developing, implementing, and sustaining training and doctrine for West Point cadets, military and civilian's employees. There is no additional cost to West Point to implement this goal since the costs associated with this mitigation strategy are absorbed by the Department of the Army and the Department of Defense (AR-25-2). Software $685,300.00 + Personnel $260,543.00 + Training (No Cost) + Maintenance $20,000.00 = Total $965,843.00.

The US and West Point must continue to improve both its defensive and offensive cyber capabilities. Aggressors both on US soil and from around the world will continue to conduct cyber-attacks against the US and some or many of these attacks will be successful. The US must constantly improve its defense and reassess cyber warfare strategies to counteract these attacks. By continuing to develop cyber capabilities, the US will be able to neutralize or at least minimize the damage of cyber-attacks from those wishing to harm the country and its infrastructure. This will help maintain and hopefully improve the high standard of national security that the US enjoys.

West Point has been and will continue to be a target for cyber criminals due to its national profile and military background. Computer networks are constantly being targeted by domestic and international organizations. The NEC West Point and the Army recognize the threat posed by cyber criminals and have implemented appropriate technical and procedural countermeasures aimed at detecting, preventing, reporting and responding to attempted network intrusions. Providing training and raising security awareness is a critical part of IT incident prevention. All organizations with access to the network should design effective training

programs and communication vehicles to help personnel understand why control methods are required, ideas they can use to reduce risks, and the impact on the organization if control methods are not incorporated.

In order to produce analysis that is credible to those who must use its results, a methodology must adhere to the recognized methods of the professional disciplines that are relevant to the method of analysis (e.g., Information Technology, engineering etc.), and it must reasonably and adequately address the concerns raised by the three groups who may be directly affected by the decisions based on its results: governments at all levels, the Critical Infrastructure and Key Structures (CI/KR) workforce, and the West Point community at large (NIPP).

References

Anonymous (Network Enterprise Command (NEC), personal interview with author, January 2012.

Army Regulation 25–2, Information Management: Information Assurance. Retrieved from http://www.apd.army.mil/pdffiles/r25_2.pdf

(CPOL) Civilian personnel On Line. Fully Automated System for Classification (FASCLASS). Retrieved from https://acpol2.army.mil/fasclass/search _fs/search_fasclass.asp

Davies, Barry, Terrorism: Inside a World Phenomenon, Virgin Books Ltd. (2005).

FBI**.** U.S. Department of Justice**:** Terrorism 2002-2005. Retrieved on 19 January 2012 from http://www.fbi.gov/stats-services/publications/terrorism-2002-2005

FoxNews.com (Aug 2011) Massive Global Cyberattack Targeting U.S., U.N. Discovered; Experts Blame China. Retrieved from http://www.foxnews.com/ scitech/2011/08/03/massive-global-cyberattack-targeting-us-un- discovered -experts-blame-china/

Harris, Shane. (Jan 2011) China's Cyber-Militia: Chinese hackers pose a clear and present danger to U.S. government and private-sector computer networks and may be responsible for two major U.S. power blackouts. Retrieved from http://www.nationaljournal .com/magazine/china-s-cyber-militia-20080531

Lewis, Ted G. Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation , John Wiley & Sons Inc. (2006)

Lynn, William J. III. (Oct 2010). Defending a New Domain: the Pentagons Cyber Strategy. Retrieved from http://www.foreignaffairs.com/articles/66552/ william-j-lynn-iii/defending-a-new-domain

MacAfee Customer Service representative. Phone conversation with business(1-888-847-8766). December 2011.

National Infrastructure Protection Plan (NIPP). Retrieved from http://www.dhs.gov/files/programs/editorial_0827.shtm

National Strategy for the Physical Protection of Critical Infrastructures and Key Assets Retrieved from http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf

Presidential Decision Directive -63. Retrieved from http://www.fas.org /irp/offdocs/pdd/pdd-63.htm

Table 1 National Institute of Standards and Technology. Stouffer, Keith, Joe Falco, Karen Kent. Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security; Special Publication 800-82. Retrieved from http://www.securitymanagement.com/archive/library/nist_scada0107.pdf

Table 2. Adversarial Threats to IT Systems. (Source: Government Accountability Office (GAO), Department of Homeland Security's (DHS's) Role in Critical Infrastructure Protection (CIP) Cyber security, GAO-05-434 (Washington, D.C.: May, 2005). Retrieved from http://www.gao.gov/new.items/d05434.pdf

Chapter 11

Planning and Preparing for Surge during special events:

Special Topics in Homeland Security

"Americans rightly asked, if this is the way our government responds to a natural disaster it knew about days in advance, how would it respond to a surprise terrorist attack? How would it respond to an earthquake?"

Russ Carnahan

"If we had a terrorist attack, the way the people respond is going to determine whether that attack is just a tragedy or whether that attack becomes an all-out disaster".

Patrick J. Kennedy

Introduction

Over the past two decades, our nation has been faced with some of the worst disasters in our history. These have ranged from natural disasters, terrorist events, and biological attacks. In order to respond to and recover from these events our nation has seen the need for vast improvements in our emergency preparedness and response capabilities. In striving to achieve these improvements there has been a large amount of education and training provided to the emergency services field. Much of this education, funding and training was aimed at the fields of Fire, Emergency Medical Service (EMS), and Police. In addition to the training, new technology is being created in order to meet the needs and prevention of another potential disaster.

This master's project identifies the potential threat of an attack during special events hosted by the United States Military Academy at West Point; specifically Graduation Ceremonies and Home Football Games, and why it is considered popular a target. This project is designed to help emergency managers realize the true potential of an attack; the potential is there as well as the threat. Since this is a relatively new topic of concern much more research must be done to fully understand how an attack of this magnitude would affect our daily operations.

Emergency response and evacuation of spectator sport venues present complex, multi-faceted problems that requiring intense preparation and coordination between emergency services, event staff, local government, and transportation or logistical departments. Additional dimensions further complicate the problem at the United States Military Academy at West Point. These include restrictive terrain, military installations, and protection measures for the Corps of Cadets and other high risk targets (DHS 2009).

Disasters Defined

A disaster is a sudden, calamitous event that seriously disrupts the functioning of a community or society and causes human, material, and economic or environmental losses that exceed the community's or society's ability to cope using its own resources. Though often caused by nature, disasters can have human origins (IFRC). According to Mr. Frederick C. Cuny; a disaster is "A situation resulting from an environmental phenomenon or armed conflict that produced stress, personal injury, physical damage, and economic disruption of great magnitude."

Disaster management is the actions taken by an organization in response to unexpected events that are adversely affecting people or resources and threatening the continued operation of the organization. Disaster management includes the development of *disaster recovery plans,* for minimizing the risk of disasters and for handling them when they do occur, and the

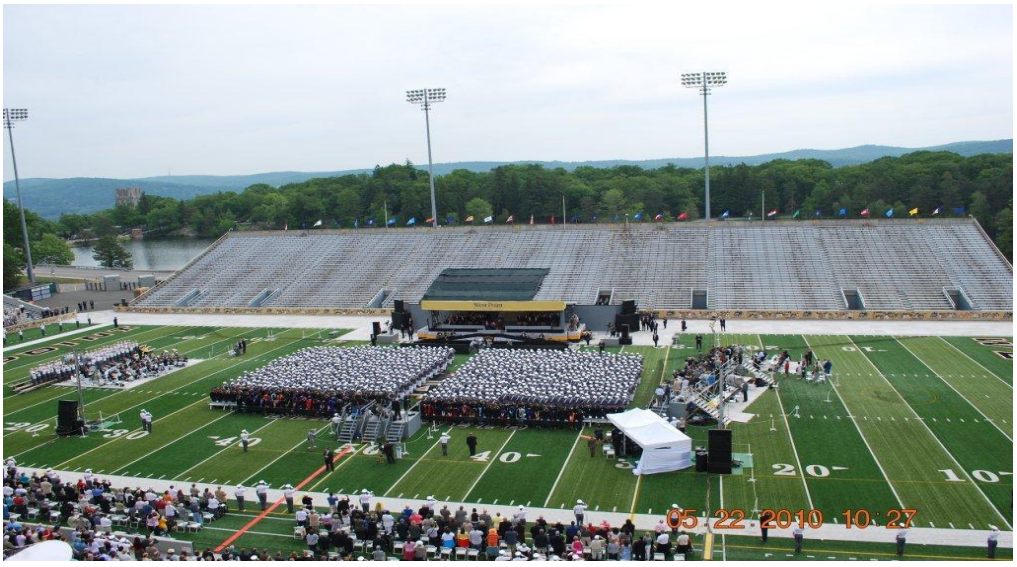
implementation of such plans (). Mitigation is the cumulative efforts taken to reduce the risk and vulnerability which a society faces. It can reduce the severity or frequency of the emergency or disaster and be implemented prior to a disaster or after a disaster (). Disaster is not necessarily defined as a destructive force in a community. If communities had mitigated the risk and were better adapted, some natural phenomena would not be so damaging or disastrous. Actively engaging in risk mitigation is an underutilized yet extremely potent means to preventing disaster, enhancing response, and saving money. An extremely important strategy to mitigating risk to disaster is the development and maintenance of Incident Command Systems (ICSs) because optimizing the efficiency and effectiveness of response efforts is a strong form of mitigation. Proper implementation of ICSs has and will save lives.

Medical Disaster

A medical disaster is one in which the destructive effects of natural or manmade forces overwhelm a community's ability to properly allocate existing resources. Disasters have the potential to cause human death and suffering, permanently transforming the character of the affected community (MEDCOM). With the media providing continual live coverage of a disaster, the rest of society is brought into closer contact with the event. Natural disasters (floods, earthquakes, hurricanes, and tornadoes) still occur with striking regularity. More frightening, however, is the growing destructive character of manmade disasters, such as chemical explosions, nuclear meltdowns, and acts of terrorism. Terrorists in particular are now more willing and able to use weapons of mass destruction (WMD) against civilian targets. These deliberate attacks of aggression are likely to produce mass casualties that will stress and potentially overwhelm a community's medical infrastructure. Examples include the bombings of the World Trade Center in New York and the Murrah Federal Building in Oklahoma City, and

the sarin nerve agent attack in Tokyo. In all of these instances, healthcare personnel were depended upon to alleviate suffering, allocate "limited" medical resources, and bring order to a potentially chaotic environment.

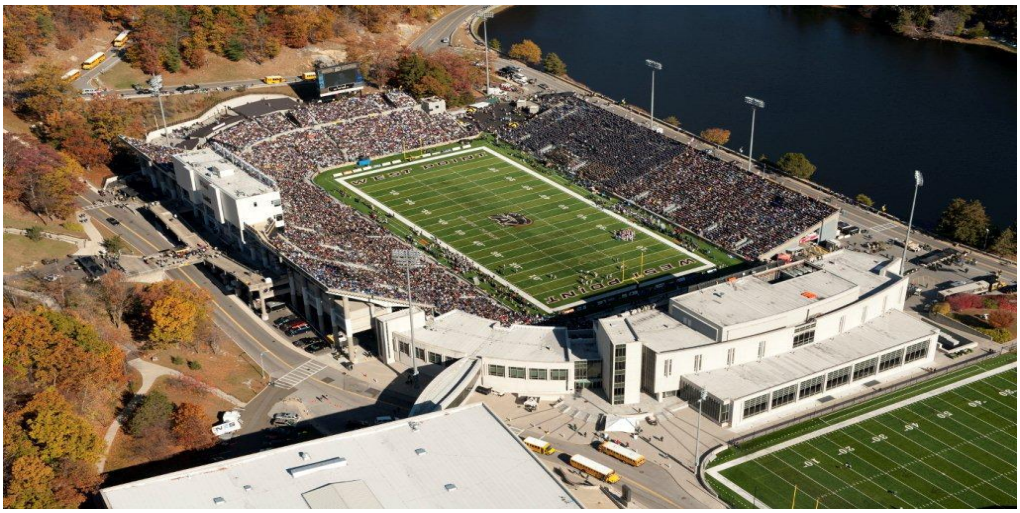
When you talk about emergency response, Fire, EMS and Police are the areas that most people think of. Although, when you focus on only these agencies you are missing an important aspect of the emergency response process. The important part which is missing in that thought process is the end point of the patient, which is the hospital. After the responding agencies work to rescue, and stabilize the patients who were involved in the event they need to take them to the hospital for further treatment. Hospitals and especially the emergency departments are as much a part of the emergency response as the other agencies mentioned above.



(Photo 1)

Graduation Week activities provide West Point with the opportunity to showcase its mission to our Nation. Annually during Memorial Day weekend; traditionally brings a large number of visitors to West Point which has the potential to strain resources (both at West Point and in Highland Falls). In addition, security precautions for the guest speaker or unknown VIP

guests may require steps that cause temporary inconvenience to guests and our neighbors in the surrounding communities. Graduation Week is the culmination of the 47-month experience by which West Point produces new junior officers for the United States Army. It is also another primary opportunity to showcase West Point and the U.S. Army not only to the US National and DoD senior leaders, but also to the American public as a whole.



(Photo 2)

Additionally Army football games showcase West Point; its football team, the installation, the community, and the United States Army. Army home Football (FB) games are high-profile events that occur on West Point each year that bring thousands of fans and distinguished visitors onto the Installation to experience a day of Army Football. Thus, the safety and security of the West Point community, our facilities, visitors, and fans is paramount. All necessary force protection, traffic and parking control measures and activities prior to, during and subsequent to each home FB game and various events that occur throughout the week leading up to a home game are carefully planned, coordinated, executed and then assessed.

Threat assessment

West Point is exposed to many hazards, all of which have the potential to disrupt the West point community, cause damage, and create casualties. Knowledge of these hazards, their frequency, and the Installation's vulnerability to them, and the capabilities in place to address them allows the community, emergency managers, and installation activities to better assess and mitigate their risks and, should an incident occur, to respond and recover from their consequences. Repeatedly the Department of Homeland Security has issued warnings on Sports Arenas. The Department of Homeland Security and the FBI issued an assessment, called "Potential Threats to Popular Sports and Entertainment Venues," that said arenas and stadiums are attractive "potential targets during events" (MSNBC). International terrorist organizations, particularly those subscribing to al-Qaida's ideology, view sports and entertainment venues and large crowds in the surrounding area as potential targets, but Intelligence agencies lack indications of current attack planning involving these locations and events. The attack methods terrorists are most likely to use against these locations and events are improvised explosive devices (IEDs) and vehicle-borne improvised explosive devices (VBIEDs). Domestic terrorist groups do not present a significant threat to U.S. college sports and entertainment venues and surrounding areas. Domestic terrorists have attacked soft targets in the past, however, and some probably continue to view major sporting events in large stadiums and associated events in surrounding areas as possible targets (MSNBC).

A risk and vulnerability assessment is a crucial step and the basis for developing a plan that defines the mission, goals, and objectives (Lewis). Based on the individual hazard profiles and the risk assessments contained below, the following hazards were assessed as most significant for West Point during special events (Lewis):

	PROBAILITY			CONSEQUENCES			PREPAREDNESS			WARNING			RISK
	HIGH	MED	LOW	MAJOR	MODERATE	MINOR	POOR	FAIR	GOOD	MINIMAL	MODERATE	ADEQUATE	VALUE
Score	*3*	*2*	*1*	*3*	*2*	*1*	*3*	*2*	*1*	*3*	*2*	*1*	
NATURAL STORMS													
Winter storms	*3*					*1*			*1*			*1*	*6*
Spring and summer		*2*				*1*			*1*		*2*		*6*
HUMAN-CAUSED													
Aircraft crashes													
Active shooter			*1*	*3*					*1*		*2*		*7*
Insider-Threat		*2*		*3*					*1*	*3*			*9*
Terrorism (General)			*1*	*3*					*1*	*3*			*8*
Hazardous Materials			*1*		*2*				*1*		*2*		*6*
NATURAL or HUMAN													
Epidemic/Pandemic influenza			*1*	*3*					*1*		*2*		*7*
Radiological emergencies			*1*		*2*				*1*			*1*	*5*

Moderately High Hazard

Terrorism in general since 9/11, has been viewed as a significant threat to the United States. Terrorists continue to aggressively recruit, train, and plan against high-value US targets with the aim of producing mass casualties, visually dramatic destruction, and fear. Given its symbolism, West Point represents a high-value target for extremist groups and individuals.

Aircraft crashes – although assessed as a low probability—represent a potentially high consequence event. The most obvious hazard is of course the loss of lives, both on board the aircraft and on the ground. Additionally, there is the potential of significant property damage from the impact and the potential fire and explosion hazard associated with unspent jet fuel. There also exists the possibility that West Point's emergency response capabilities could become quickly exhausted.

Active shooter incidents pose unique concerns for all facets of a community. A number of tragic shooting incidents in public spaces, campuses, and now at a military Installation have heightened the concern and need for preparedness for this potentially high consequence event. Moreover, there are a multitude of issues and emerging threat scenarios that make preparing for, responding to and recovering from an active shooter incident more challenging than other incidents.

Hazardous Materials (HAZMAT) incidents of varying proportions could happen anytime and at any place on or nearby the Installation and result in a fire, explosion, toxic cloud, or direct contamination of people and property. Health problems may be immediate, as from corrosive effects on skin and lungs, or be delayed, such as cancer from a carcinogen. Damage to property could range from immediate destruction through explosion to long-term contamination by a persistent hazardous substance.

Moderately Low Hazard

Spring and summer storms, a common hazard in the Hudson Valley, are usually characterized by strong winds, are frequently combined with heavy rain and dangerous lightning. Excluding winter weather events, this category of storms includes thunderstorms, hailstorms, hurricanes, and tornados.

Winter storms can range from a moderate snow over a few hours to a blizzard with blinding, wind-driven snow that lasts for several days. Many winter storms are accompanied by dangerously low temperatures and sometimes by strong winds, icing, sleet, and freezing rain. Epidemic/Pandemic influenza represents a dangerous threat and formidable response challenge to West Point. Given the unpredictable behavior of viruses, neither the timing nor the severity of the next pandemic and its impact on West Point can be predicted with any certainty.

Radiological emergencies at the nearby Indian Point nuclear power plant may place West Point at risk for exposure to or ingestion of radiological contaminants. While the probability of a catastrophic hazardous material release occurring is very small, the consequences from radiological materials could be significant. Equally significant with potential devastation consequences could be a chemical or biological incident.

It is important to note that hazards occur in varying degrees, and seldom is there a boiler-plate response to an incident. With a unified response from West Point authorities and mutual aid partners, the strategies outlined in this project should facilitate an appropriate and timely all-hazards response. The West Point community will be best served by a program that emphasizes risk assessment and mitigation, and that maintains the authority and versatility to make prompt and appropriate decisions in times of crisis that will minimize not only the potential for injury or death, property damage or destruction, but uphold the reputation and integrity of West Point. In order to create and maintain a viable emergency readiness, response and recovery posture there must be a high level of understanding and consistency of thought among all participants.

Existing Plans and Framework

"The National Response Framework (NRF) is the overarching guide to how the nation conducts all hazards response. It is built on scalable, flexible, and capital coordinating structures to align key roles and responsibilities across the nation (NRF, 2008)." In short, the NRF is somewhat of a playbook for elected officials and emergency managers other practitioners and policymakers at all levels. It also has applicability to 1st responders and their leadership as a guide to help them effectively integrates with other levels of response within the government. NIMS provides a systematic, proactive approach to guide departments and agencies at all levels of government, nongovernmental organizations, and the private sectors to work seamlessly to prevent, protect against, respond to, recover from, and mitigate the effects of incidents, regardless of calls, size, location, or complexity, in order to reduce the loss of life and property and harm to the environment. (Chertoff, 2008) the foundation of all of those plans is the West Point Emergency Management Plan (WPEMP), it has been developed to provide a basic procedural outline for hazard mitigation, preparedness, response, and recovery at West Point.

West Point has a variety of Emergency management plans that have been authored but have not all been exercised and evaluated. The West Point Emergency Management Plan (WPEMP) is a basic source of reference considered necessary to accomplish the various types of emergency missions. It is designed to bring the user to the point of knowing what is to be done, and who is to do it. It may include information relative to when and where the response will be effective, and even why it will be done. However, each participating organization must depend upon its own expertise to develop the procedures for carrying out its assignments in support of this plan.

The West Point Emergency Management Plan (WPEMP). Is an all-discipline, all-hazards document establishes a comprehensive framework for the management of installation-wide incidents. Incident Annex A (Antiterrorism Plan) to the WPEMP. This plan establishes security measures to protect the Corps of Cadets; safeguard personnel and property and control access to the installation and mission essential vulnerable areas on West Point. This plan also provides phased security upgrades and antiterrorism measures to meet terrorist, criminal, dissident, and sabotage threats. However there is no plan or Annex that addresses medical surge. Inherent to all plans are:

Mitigation measures and practices to reduce the risks and vulnerabilities associated with a potential hazardous situation impacting the stadium. These preventative measures include hazard identification and vulnerability analyses, situational awareness (e.g., intelligence analysis and dissemination), public education, and security and safety assessments.

Preparedness plans, procedures, and capabilities to enable a satisfactory level of readiness to respond professionally to all hazards. These measures include evacuation training and exercises for decision-makers, first responders, stadium staff, command and control elements,

and mutual aid partners; implementation and testing of warning and notification systems; confirmation of resource inventories and plans for their sustainment and deployment; formalized and tested mutual aid agreements; and a public information and education campaign plan (DHS 2007).

Response capabilities - as soon as a threat is detected it involves mobilizing and positioning emergency equipment; getting people out of danger; providing needed food, water, sanitation, shelter and medical services; and bringing affected services and systems back on line. Keeping mutual aid partners and higher headquarters informed and initiating long-term planning are included within this phase. When the incident exceeds West Point's capabilities local, regional, State and Federal assets would need to be requested (DHS 2007).

Recovery activities that seek to restore normal operations after the immediate needs of the response phase have been met. Recovery efforts are concerned with issues and decisions that must be made after immediate needs are addressed and serve to inform the next phase of mitigation planning (DHS 2007).

Special Considerations

Preparing to respond to CBRNE incidents is very similar to contingency planning undertaken for other types of manmade or natural disasters, as long as the unique characteristics of a attack are considered (as discussed earlier). Pro-active and integrated planning, coordination, training, and realistic drills will allow each community to respond to these events in an organized, efficient manner, using available Federal, state, and local resources. Successful disaster planning requires hospital personnel to be familiar with the local incident management system, standard operating procedures (SOPs), triage, and personal protective equipment (PPE) (HSEEP). A disaster plan, however, is only as effective as the assumptions on which it is based.

Unfortunately, many medical disaster planning initiatives are based on misconceptions. As a result, many disaster plans prove to be ineffective in actual use (MEDCOM).

In the hospital, disaster planning has traditionally been compartmentalized depending on the type of disaster. For example, one plan is created for external disasters, another for HAZMAT accidents, and a completely different plan for natural disasters (AR 40-61). The end result is often a confusing and cumbersome disaster-planning document that is unfamiliar to hospital personnel. Proficient disaster planning requires a unified, "all-hazards approach" to disasters that are likely to occur in the community. This standardized plan can be expanded or contracted depending on the situation.

Readiness Phase - In preparing to respond effectively to a CBRNE disaster, hospitals must take an inventory of their current capabilities. Hospital personnel must be made aware of the overall disaster plan, which must be acted out realistically in disaster drills (DHS 2007). The plan must address how increased numbers of patients will be triaged, decontaminated, and treated. If training, equipment, or supplies are lacking in specific areas (such as, antidotes, decontamination, PPE, data tracking, etc.), these deficiencies must be rectified (AR 40-61).

Planning Phase - Incorporate all responsible individuals and departments into the planning process. Keep the plan simple and cost effective, and assign tasks to individuals that parallel their normal daily activities. Plan for problems that are most likely to occur in any disaster, and develop policies and procedures to address them. Examples include: Communication problems between the triage area, the ED, and the command center; Coordination and sharing of information; Triage, victim tracking, and decontamination; and Staff rotation to minimize fatigue and stress (USAMRICD/DHS 2007).

Participate in joint planning**.** EMS, law enforcement, and hospital disaster planners need to work together to develop an organized approach to disasters and mass casualty events. To be successful, pre-hospital and hospital disaster plans need to be effectively integrated into the community disaster plan. This planning may be best accomplished through existing committees, such as the Local Emergency Planning Committee (LEPC), or in association with the local fire chief and local emergency management officials (MEDCOM).

Develop mutual aid agreements**.** Hospitals and EMS providers should jointly develop mutual aid agreements concerning patient transport, hospital transfers, and sheltering during a mass casualty situation. Anticipating that the closest hospitals to the incident will see the majority of casualties, EMS should transport the less severely injured patients to outlying medical facilities to help ensure adequate medical care to all disaster victims Army Pamphlet).

Develop policies and procedures**.** Formulate policies and procedures that address staff safety and personal protection, and standardize the hospital's approach to identifying, decontaminating, and treating contaminated victims (MEDCOM/AR 40-61).

Acquire necessary equipment**.** Obtain PPE and decontamination equipment and train frequently utilizing this equipment to protect the safety of hospital providers (AR 40-61).. All training and materials used must conform to OSHA regulations (OSHA). Routine protective gear (such as goggles, surgical facemask, gloves, and gown) may not offer sufficient protection in all circumstances (such as in the case of a nerve agent attack). Levels of PPE will be determined by the local jurisdiction in concert with OSHA regulations (OSHA).

Stockpile antidotes**.** Develop adequate caches of antidotes that are readily available to quickly and accurately treat victims of a chemical attack. EDs should maintain basic treatment guidelines for the types of CBRNE events likely to be seen. Summarizing this information on

treatment cards or posters helps to regularly reinforce the information while streamlining the delivery of medical care (Hunt).

Recovery phase - During recovery, the focus of disaster response shifts away from the acute injuries and illnesses caused by the disaster to the everyday needs of the general population. The impacted population may have increased needs for medication, shelter, food, water, clothing, and emotional support that must be addressed. Hospitals must also contend with the emotional needs and fatigue of their own personnel (Army Pamphlet).

Training

All hospital emergency departments should have the capability to treat contaminated patients from everyday hazardous materials accidents. Preparedness begins with OSHA hazardous materials Awareness and Operations training that is specific to the hospital environment. Training needs to include respiratory fit testing, donning and doffing of personal protective equipment, proper decontamination procedures, incident management, triage, and mass casualty patient care after a hazardous materials incident. Once this foundation of training is established it should be expanded to include CBRNE agents (USAMRICD).

Personal Protective Equipment (PPE)

Personal Protective Equipment refers to the use of protective clothing (suits, boots, gloves,) eye protection, and respiratory equipment that is designed to protect the eyes, lungs, and skin of the responder. During a HAZMAT accident or incident involving CBRNE agents, hospital personnel must be protected from the risk of personal injury (OSHA/. These individuals must be provided PPE and trained in its use after first receiving medical clearance from a physician or licensed health care professional, and provided appropriate fit testing of the respirator they will use. Retraining in the use of PPE needs to be provided at least annually to

ensure staff proficiency. The level of PPE required for healthcare providers and support staff will vary depending upon their risk of exposure and assigned responsibilities during a CBRNE incident. Many hospital personnel directly involved in the decontamination of victims will find Level B protective gear (including an atmosphere-supplying respirator) sufficient for such tasks, but the proper level of protection must be tailored to the hazard involved (OSHA). If the hazardous material has been identified, and its air concentration measured and determined to be below an immediately dangerous to life and health toxic level, PPE levels may be adjusted by the incident commander to level C or lower (OSHA). Standard universal precautions should be followed by all other personnel when interacting with patients who have already completed the decontamination process. In addition to following Federal guidelines for protective equipment use, responders must comply with any applicable state and local regulations.

Biological Self Protection

The best safeguard to prevent the spread of a biological agent is self-protection. The first responder and medical caregiver must treat every patient with respiratory complaints (fever, cough, and shortness of breath) and open wounds as a possible infectious source. All health care providers should wear eye protection and follow standard universal precautions when treating these patients (FM 284). Special protective garments are generally not required since hospital isolation clothing or disposable gowns provide reasonable protection against skin absorption. In areas where a biological agent aerosol could be generated, a higher level of respiratory protection may be required (MEDCOM).

PPE – Self Protection from Radiological Materials

The proper method of self-protection from radiological hazards depends on the specific hazard encountered. If the primary danger is from contamination by radioactive particles or dust,

proper patient handling will prevent re-suspension and possible health effects. Radioactive debris can be harmlessly washed from the surface of the body, but inhalation of the same material can lead to internal contamination and incorporation. Irradiation presents a different hazard to responders. The protection principles of time distance, shielding, and amount of radioactive material should be considered. While standard PPE will provide protection against external alpha and most beta radiation sources, normal protective clothing is ineffective for radioactive sources emitting gamma or neutron radiation. Dense shielding is not likely to be available for emergency treatment of casualties at the average hospital. Decisions to commit individual facility resources to radiological hazards must be based on local protocols and the hospital's emergency response plan. It is important to note that the wear of a dosimeter will not protect you from the effects of radiation, but will document your exposure to penetrating radiation (AFRRI).

Decontamination

Decontamination is the physical process of removing harmful substances from personnel, equipment, and supplies. It should be performed whenever there is known or suspected contamination with a hazardous substance. Limiting the spread of contamination into the hospital is accomplished by preventing the contaminated individuals from entering the medical facility (USAMRICD). In addition, hospitals must ensure that healthcare personnel wear personal protective equipment, and that the institution has the capacity to perform decontamination, with a plan for managing the resulting wastes and runoff. Caregivers who do not have PPE should not attempt to treat un-decontaminated casualties. Before working on the next potentially contaminated casualty, caregivers should perform a quick wash-down of areas that were in contact with the previous victim. This will prevent "cross contamination," the

transfer of hazardous substances from one casualty to another. Merely removing the victim's clothing will eliminate about 80% - 90% of the contamination. Gently scrubbing the body surface with soap and a soft brush helps to remove fat-soluble chemicals and solid materials remaining on the skin (MEDCOM).

Victims of a CBRNE incident who have been fully decontaminated at the scene (clothing removal and showering) do not require additional decontamination at the hospital. These patients can be brought directly into the hospital for further evaluation and treatment. Individuals, who only had their clothing removed at the scene, were exposed to an aerosol or vapor, and their symptoms are minimal or improving, may also be brought directly into the hospital without the need for further decontamination. Victims arriving at the hospital with an unclear exposure history who are symptomatic from a CBRNE agent (or hazardous materials) should be fully decontaminated with soap and water before entering treatment areas. Victims in extremis require rapid decontamination which includes quickly removing the patient's clothing (using scissors) and flushing the skin with copious amounts of water (Medical Management).

Staff Preparedness

The medical needs of the unaffected community must be considered since these requirements will not diminish in the event of an MCI or CBRNE event. Plans must include provisions for diverting the normal number of trauma and medical emergency patients to other facilities, possibly in neighboring communities (MEDCOM). These surrounding hospitals must be consulted during the planning phase, so they in turn can make realistic plans regarding the most efficient use of resources after a major terrorist event. In addition to planning and training, hospital staff will need to be "mentally" prepared to deal with the ramifications of a large scale terrorist incident. If a disaster does occur in the community, staff members will want to remain

at the hospital for the duration of the crisis to offer assistance. Although their desires are admirable, some of these individuals will need to return home so personnel can be rotated effectively to prevent staffing congestion and help minimize fatigue (MEDCOM).

Logistics/Supplies

A major challenge of any disaster response is gathering, organizing and moving supplies to the appropriate area. Within a hospital environment, the same condition applies. Asset management, both, within the hospital and through mutual assistance with other facilities or agencies, may prove to be the decisive factor in whether a hospital conquers a mass casualty event or is overwhelmed by it. During a mass casualty event, hospitals generally require increased access to several components of care and response, including: Personal protective equipment; Medications, antidotes and vaccines; and Ventilators (AR 40-61)

Maximal Utilization of Hospital Space

Alternative medical treatment areas could be identified to help prevent overwhelming the hospital's resources, especially those in the emergency department. These alternative sites may be internal (the cafeteria, auditorium, outpatients clinics, etc.) or external (schools, sporting facilities, other athletic facilities, etc.) to the hospital (Hunt). In addition, an MOA could be established with the local Department of Transportation or busing company to help assist in victim transport. Plan to use all available space. An important way to maximize the existing resources at your hospital is to make space usage a part of the overall disaster planning process. Because response to CBRNE could thrust extraordinary demands on a healthcare institution, the timely response to a wave of victims could hinge partly on pre-designating suitable areas of the hospital for specialized functions. Large exterior open areas might be perfect for external decontamination, while large indoor areas could serve as patient holding and re-triage centers.

Isolated areas with controlled access could function in additional specialized roles, such as overflow treatment areas for biological casualties; and for security and efficiency reasons, the hospital's command and control functions could also be overseen in a secure area (Hunt). An additional space planning issue already addressed in many disaster plans is designation of temporary morgue facilities to serve as a secure holding site for the least fortunate victims.

Conclusion

West Point like any other small community is susceptible to incidents that can produce mass casualties that include, but are not limited to: Multiple vehicle, passenger bus, or troop carrying vehicle incident; Building collapse; Aircraft accident; Hazardous Materials (HAZMAT) incident; Pandemic/epidemic, CBRNE; or criminal/terrorist act. Mutual aid agreements need to be an organized, coordinated, reciprocal agreement in which all emergency medical providers plan for and effectively carry out emergency response where needed. Personnel and equipment of all participating emergency medical service providers, regardless of type and size, are employed for the purpose of providing emergency medical assistance. In times of need, due to excessive EMS call volume, vehicle break down, lack of available proper local manpower, advanced life support intervention, or mass casualty incident.

The National Training Program (NTP) provides a planned approach to training for emergency managers and emergency response providers across the nation that supports the National Preparedness Guidelines. FEMA has several training organizations that are heavily engaged in preparing the nation's responders and emergency management personnel. The organizations are the Center for Domestic Preparedness (CDP), Emergency Management Institute (EMI), National Training and Education Division (NTED), and the National Fire Academy (NFA). There are numerous types of training that the government receives, such as

CBRNE that has all kinds of individual types within it. Anniston, AL is home to several different CBRNE and WMD live agent training courses. Also, Ft Leonard Wood, MO is home to the Army and Marine Corps' training for their Chemical, Biological, Radiological, and Nuclear Defense personnel. The site in MO has a Chemical Defense Training Facility (CDTF) where live agent training occurs.

References

AFRRI Armed Forces Radiobiology Research Institute, A United States Department of Defense research laboratory. Retrieved from http://www.usuhs.mil/afrri/

Army Regulation 40-61, Medical Logistics Policies and Procedures. Washington, D.C.: Government Printing Office.

ARMY FM 8-284 (2000). Treatment of Biological Warfare Agent Casualties. Retrieved from http://www.med.navy.mil/directives/Pub/5042.pdf

Army Pamphlet 525-XX (Draft 2011) Army Emergency Management Program Washington, D.C.: Government Printing Office.

Chertoff, M. (2008). National incident management system. Washington, D.C.: Government Printing Office.

Department of Homeland Security, (2008). National response framework. Washington, D.C.: Government Printing Office.

Department of Homeland Security, (2007) Target Capabilities List. Washington, D.C.: Government Printing Office.

Department of Homeland Security, (2009) Threats to College Sports and Entertainment Venues and Surrounding Areas. Washington, D.C.: Government Printing Office.

Department of Labor, (2012). 29 Code of federal regulations. Retrieved from http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=standards&p_id=9765

(HSEEP), FEMA, Homeland Security Exercise and Evaluation Program. Retrieved from https://hseep.dhs.gov/pages/1001_HSEEP7.aspx. Accessed 3 May 2011

Hunt, Richard C. et al. Centers for Disease Control and Prevention (2010) Updated - In A Moment's Notice: Surge Capacity for Terrorist Bombings: Challenges and Proposed

Solutions

IFRC - The International Federation of Red Cross and Red Crescent Societies. Retrieved from http://www.ifrc.org/en/what-we-do/disaster-management/about-disasters/what-is-a-disaster/

Lewis, Ted G. Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation , John Wiley & Sons Inc. (2006)

MEDCOM Regulation 525-4, Emergency Preparedness, 9 February 2004. Washington, D.C.: Government Printing Office.

Medical Management of Chemical and Biological Casualties. Retrieved from https://ccc.apgea.army.mil/courses/distance/distance.htm

MSNBC Feds issue security alerts on stadiums, hotels Officials: More than a half-dozen people possibly in alleged NYC plot. Retrieved from http://www.msnbc.msn.com/id/32967671/ns/us_news- security/t/feds-issue-security-alerts-stadiums-hotels/

OSHA (2003) Personal Protective Equipment. Retrieved from http://www.osha.gov/ Publications/osha3151.pdf

Petrie, M. (n.d.). Homeland Security Exercise and Evaluation Program (HSEEP): Quick Reference Guide. University of California, Berkeley Center for Infectious Diseases and Emergency Readiness

USAMRICD United States Army Medical Research Institute of Chemical Defense). Retrieved from http://chemdef.apgea.army.mil/

US Army Medical Research Institute of Chemical Defense (USAMRICD). Retrieved from https://ccc.apgea.

army.mil/courses/In_house/MCBC.htm

Conclusion

The evolving threat environment has enhanced our awareness for the need for Continuity of Operations (COOP) capabilities that would enable West Point organizations to continue their essential functions across a broad spectrum of potential hazards. We remain at war with adversaries who are committed to harming our people, our facilities, and our way of life. In the midst of this conflict, West Point and the Hudson Valley region are vulnerable to emergencies that may impact life, property, and operations.

Through its force protection-related programs, the Department of Defense (DoD), Department of the Army (DA), and Installation Management Command (IMCOM) are working jointly to enhance the ability of installations to prepare for, prevent, respond to, and recover from all-hazards. An element of that improvement effort is the Homeland Security Exercise and Evaluation Program (HSEEP) that includes the Target Capabilities List, a framework to guide operational readiness planning and assessment.

The overall purpose of a COOP is to ensure the continuity of essential functions under all circumstances that may disrupt normal operations. As a baseline of preparedness for the full range of potential hazards, all USAG-West Point organizations should have in place viable COOP capabilities. Over the past several years, organizations have become increasingly aware of the extent to which emergencies can interrupt, paralyze, disrupt, and/or destroy their capabilities to perform essential functions effectively under emergency conditions.

Continuity of Operations (COOP) is the capability of an organization to continue mission-essential functions without unacceptable interruption. COOP planning includes

preparatory measures, response actions, and restoration activities planned or taken to ensure continuation of these functions to maintain military effectiveness, readiness, and survivability. Leaders have a moral responsibility to ensure the safety of their community. They also have a legal obligation to operate in a practical and efficient manner, even during an impending threat or following a crisis. To have a successful COOP plan, each agency must determine what its essential functions are by considering its mission and its personnel. Assigning priorities helps to distinguish between essential and nonessential functions.

ABBREVIATIONS

ACSIM: Assistant Chief of Staff for Installation Management

AOR: Area of Responsibility

ARNG: Army National Guard

ASCC: Army Service Component Command

AT: Antiterrorism

ATEP: Antiterrorism Enterprise Portal

ATO: Antiterrorism Officer

CA: Criticality Assessment

CBRNE: Chemical, Biological, Radiological, Nuclear, high-yield Explosive

CIDC: Criminal Investigations Directorate Command

Cbt RIF: Combating Terrorism-Readiness Initiative Fund

COM: Chief of Mission

CVAMP: Core Vulnerability Assessment Management Program

DoD: Department of Defense

FPEC: Force Protection Executive Committee

FPWG: Force Protection Working Group

FORSCOM: US Army Forces Command

FPCON: Force Protection Condition

FY: Fiscal Year

GCC: Geographic Combatant Commander

HHA: Higher Headquarters Assessment

ARNORTH: Headquarters, Department of the Army

HRB: High Risk Billet

HRP: High Risk Personnel

IMCOM: Installation Management Agency

INSCOM: US Army Intelligence Command

JCIDS: Joint Capabilities Integration and Development System

JSIVA: Joint Staff Integrated Vulnerability Assessment

MAA: Mutual Aid Agreement

MACOM: Major Army Command

MOA: Memorandum of Agreement

MOU: Memorandum of Understanding

OEF: Operation Enduring Freedom

OIF: Operation Iraqi Freedom

POM: Program Objective Memorandum

PPBE: Planning, Programming, Budgeting, and Execution

PSVA: Personal Security Vulnerability Assessment

RA: Risk Assessment

RDT&E: Research, Development, Testing and Evaluation

OSD: Office of the Secretary of Defense

RAM: Random Antiterrorism Measure

RMO: Resource Management Office

SIPRNET: SECRET Internet Protocol Network

TA: Threat Assessment

GUARDIAN: Threat and Local Observation Notice Reporting

TTP: Tactics, Techniques, and Procedures

TWG: Threat Working Group

UFC: Unified Facilities Criteria

USARC: US Army Reserve Command

WMD: Weapons of Mass Destruction