DEFENSE FOR THE COLLEGE CAMPUS

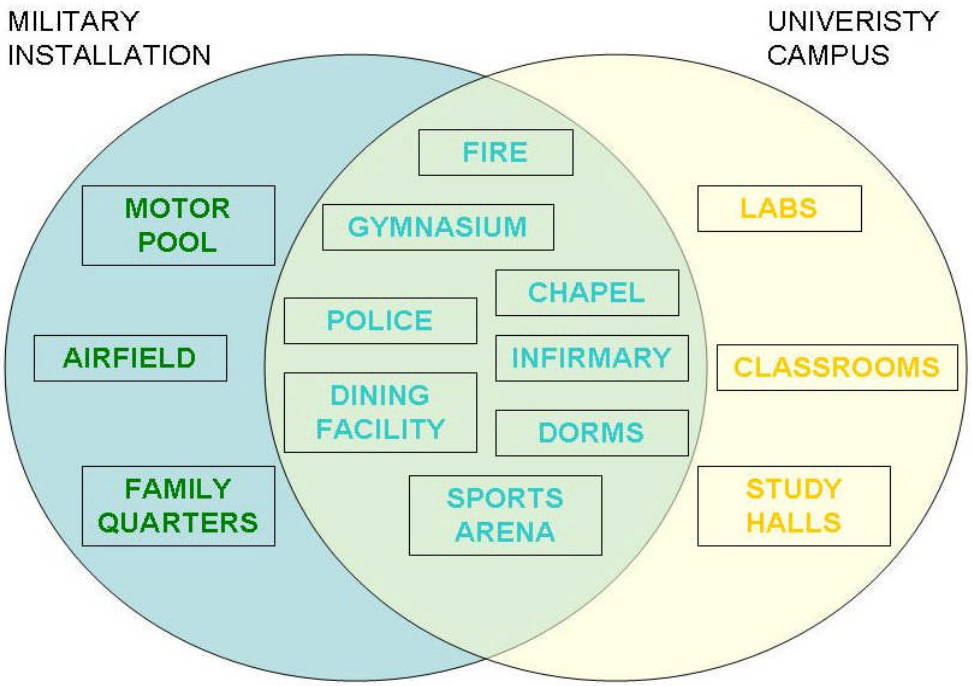
By Evelyn Byrd, CPP

Today is Monday, April 16, 2007. News reports trickle in this morning about yet another shooting on a college campus. This one, we thought, ended in a single death. We have seen similar shootings this year, in Montreal and in Seattle. We may be desensitized a bit, and life goes on.

By now, we know this was anything but "another shooting." By now, we know that on this day, the most deadly shooting rampage in modern history took place on the campus of Virginia Tech in Blacksburg, Virginia.

Protecting college campuses, and the people on them, is a tough job. Public Safety Personnel work hard and train to stay abreast of the latest and greatest methods. They develop and maintain security programs that include crime prevention, emergency response, and access control, to name a few. The challenge can be monumental.

A college campus is similar to a military installation in many ways. The US Department of Defense (DoD) has been protecting installations, and the people on them, for generations. The threat of terrorism, particularly since the bombing of Khobar Towers (Saudi Arabia) in 1997 gave birth to the Antiterrorism (AT) Standards that are used today in the US military. This article proposes that those very same AT Standards used to protect military bases can be used as a basis for a comprehensive security program on college campuses.



PROBLEM: PROTECTING COLLEGE CAMPUSES

The routine daily security duties on any campus require awareness, diligence, training and expertise. The list is endless: access control for the dining facility; protection of special collections in the library; special event security during athletic events. But what stands out most are the high profile cases, the unexpected situations where lives are lost and the media arrives.

One layer of protection to improve campus life is the crime prevention layer. In 1986, Lehigh University freshman Jeanne Clery was beaten, raped and murdered in her room on campus during the commission of a robbery by another Lehigh student. The Clery Act, passed in 1990 and amended in 1992, requires all colleges and universities to report crime on and around their campuses. This law has increased campus crime prevention and awareness significantly in the past 15 years.

Lessons learned in the aftermath of Hurricane Katrina have also been put into action at many college campuses across the country. Colleges in the gulf region were closed longer than they had ever been. As a result, continuity plans were dusted off and updated. These developments improved recovery operations, but not necessarily response efforts.

In the area of law enforcement, the Commission on Accreditation of Law Enforcement Agencies (CALEA.org) administers a program that seeks to improve public safety services. The accreditation process uses a set of professional standards, one of which requires "a preparedness program to be put in place – so an agency is ready to address natural and manmade critical incidents." This process is thorough and effective in meeting goals for law enforcement. But it is not comprehensive enough to meet the broad needs of an entire college or university community.

At this time, despite high profile incidents, there does not seem to be any national (or international) standards for prevention, response, or recovery in the campus environment. In terms of solutions, it is possible that the US Department of Education might support establishment of minimum standards. Another possibility is using the academic accreditation infrastructure to verify compliance with any future set of minimum standards.

SOLUTION: DEPARTMENT OF DEFENSE ANTITERRORISM?

The Department of Defense (DoD) has a long history of protecting people and other assets, such as sensitive information, equipment, and facilities. The core Antiterrorism Program has been in operation for over 10 years now. This program has also been developed under US military funding, and is available for use and review by security directors and managers across the country.

The most significant aspect of this program relative to campus security is comprehensiveness. Although the AT program is focused on protection from acts of terrorism, the elements and standards address almost all areas of security for a base. The

program could conceivably be used as a template to establish a security program from the ground up. It can also be used to effectively evaluate an already existing program.

Loss of life makes even the largest bureaucracy receptive to new solutions. Antiterrorism has been a high priority for all military services and commanders at every level, especially since the bombing of the Marine Barracks in Beirut in 1983. The current AT program was developed after the Khobar Towers bombing in Saudi Arabia in June 1996. Since that time, the program has improved continuously with lessons learned from the USS Cole bombing, and the attack on the Pentagon in 2001. The sense of urgency and necessity is palpable.

Five elements make up the core of the AT program: risk management, planning, training and exercises, resource application and comprehensive program review. The most recent version of the policy instruction organizes the standards into one of those five elements, or categories.

1. Risk Management

The entire program is nonlinear, and should be a continuous process. However, risk management sets the foundation for any rational security program. Risk management is not unique to the military. But in this time of limited resources, the DoD Antiterrorism Program recognizes the importance of using a deliberate, systematic approach to risk management before selecting and implementing appropriate security measures. Among the essential components in this step are: threat assessment, criticality assessment, and vulnerability assessment.

Threat assessments are required to be updated annually, tailored to local conditions, and conducted using integrated and fused information from all available resources. Assessment of threat in a college or university environment is most effective from an all-hazards point of view. Everything from terrorism (Virginia Tech) to weather (Katrina) must be considered in order to be effective.

Criticality assessment identifies which assets require the most protection. This part of the risk management process will "identify, classify and prioritize mission-essential assets, resources and personnel," if done properly. As with the other components, assessing criticality is not unique to the military. But they have a significant hand in developing the CARVER tool, and have a vested interest in the MSHARPP process as well. The criticality assessment is absolutely necessary when resources are limited.

Finally, the vulnerability assessment helps determine where those limited resources are best employed. The mandatory vulnerability assessments are outlined, including but not limited to a standardized, comprehensive process conducted by a team of experts and a more local, tailored process conducted more frequently as dictated by the mission or the threat.

2. Planning

AT Planning requires site-specific instructions tailored for each base. Responsibilities for key personnel are detailed in this phase of development. They begin at the top with a program coordinator, an antiterrorism officer (ATO), an AT working group, and an executive committee. The working group and executive committee can be replicated almost directly on campuses. The program coordinator may already exist in the position of a Public Safety Officer, or similar position. The ATO role and responsibilities may already exist if a Homeland Security Officer is present, or by creation of a new position.

Under the planning element is the requirement to meet mass notification standards with proper training, equipment, planning and exercises to validate the plans. This is an issue that will be closely reviewed as a result of the April 17th shooting on the Virginia Tech campus. The system used must be included in the plan, included in training and exercises, and tested regularly.

One of the most cost effective solutions within the DoD AT program is Random Antiterrorism Measures (RAM). Random use of security measures, according to the instruction, maximizes the deterrence value by varying time, place, and other variables. This makes planning any threat attack more difficult.

Planning also requires establishment of a uniform system of both preventive and pro-active actions and responses to identified threats. This set of discrete, predetermined levels gives the senior responsible party a tool to implement appropriate protective measures for any situation. This set of measures is written and reviewed by the working group, approved by the committee, and validated through exercises, thereby reducing the risk and response time.

Other transferable components under the heading of planning include using appropriate physical security measures, protecting off-base facilities and activities, and specific measures for special or critical assets. Off-campus facilities might include housing areas and sports arenas. Special or critical assets on campus might include special collections in the library, museums, or even the office of the university president.

3. Training and Awareness

Emphasis on training and awareness should come from the highest echelons in any organization. DoD requires training on several levels. The first is 100% awareness training, with different frequency requirements for various subgroups. The first level of training should also include site-specific information tailored for each facility.

The second level, and longest in duration, is for the ATO as primary advisor and responsible developer of the installation plan. The third and fourth levels are for senior leaders from a “big picture”, wide area focus. These two levels might be combined for senior administrators on a college or university campus. Overall, this structure is easily transferable to the college campus establishment.

Exercising the overall plan, or elements thereof, is an absolute necessity for any functional security program. Military installations ensure that exercises are conducted often, are realistic, and integrated with as many players, organic and external, as there are in the plan. These features are not unique to DoD AT, and appear to be an existing strength within university police and security forces.

4. Resource Application

Resource Application is unique to the organization at hand and will not be discussed in depth here. One point worth making is that a single, coordinated system to document, prioritize and monitor the status of requests for resources can be highly effective.

5. Comprehensive Program Review

Finally, a comprehensive program review rounds out the elements necessary for a good overall antiterrorism, or security, program. Again, this requirement must be tailored to meet site-specific needs of each college and university. But some key factors include frequency of reviews, composition of review teams, and benchmarks or standards used.

SUMMARY

Whether it is under public safety, security forces or law enforcement, the responsibility to protect campuses is under more pressure than ever before. Personnel tasked with security duties need every effective tool to be successful. After paying the high price of lost lives, the US Department of Defense has developed an effective program to protect all assets from terrorism through the Antiterrorism Program. This AT program has much to offer college and university campuses and those responsible for their security.

CONCLUSION

Military installations and college/university campuses have similarities. Both are identified by geographic boundaries, and mission-based with a common purpose. Also, some of the facilities are virtually identical: dormitories/barracks, dining facilities, athletic/recreation centers, libraries, chapels, etc.

Time will tell if this theory is accurate. After initial review, it stands to reason that campuses can benefit from most of the elements of the DoD AT Program. The program can be used as a template to create a comprehensive security program for campuses, where one does not already exist. It can also be used to review an existing program.

****

Evelyn Byrd has over 25 years in the security field, including 15 years in the US Army. She has extensive training and experience in Security Management and Antiterrorism/Force Protection (AT/FP). As a government contractor and civil servant, she has supported AT/FP programs for US Army Reserve Command, US Army Chemical Materials Agency, US Army Garrison Japan, and Commander, Naval Installations.

Evelyn Byrd, C.P.P.
certified protection professional