The Source for Antiterrorism Information

SPRING 2012 | Volume 14 | Issue 1

THE GUARDIAN
ANTITERRORISM JOURNAL

FINAL ISSUE

10 years of providing critical AT/FP information to troops at home and abroad

A Joint Staff, Deputy Directorate for Antiterrorism/Homeland Defense, Antiterrorism/Force Protection Division Publication

The Pentagon, Room MB917 | Washington, DC 20318

The Guardian
The Guardian is published for the Chairman of the Joint Chiefs of Staff by the Antiterrorism/Force Protection Division of the J-34 Deputy Directorate for Antiterrorism/Homeland Defense to share knowledge, support discussion, and impart lessons and information in a timely manner.

Antiterrorism Quotes

23 February 2012

"Geopolitical cycles will change, and these changes may cause a shift in who employs terrorism and how it is employed. But as a tactic, terrorism will continue no matter what the next geopolitical cycle brings."

—Scott Stewart, stratfor.com.

30 January 2012

"Last year, I had the honor of attending the opening of the new 9/11 memorial in New York City. That memorial, like the one at the Pentagon and in the fields outside Shanksville, Pennsylvania, stands as a reminder of those we lost and will never forget. But these memorials must serve another purpose. They must stand as reminders of our need for vigilance in a dangerous world and as a symbol of our resilience as a nation—a nation that has proven time and again that we will always come back stronger from tragedy and adversity."

—Secretary of Homeland Security Janet Napalitano, Second Annual Address on the State of America's Homeland Security: Homeland Security and Economic Security.

15 February 2012

"Last year, the NATO effort in Libya also concluded with the fall of Gadhafi, and successful counterterrorism efforts have significantly weakened al Qaeda and decimated its leadership. But despite what we have been able to achieve, unlike past drawdowns where threats have receded, the United States still faces a complex array of security challenges across the globe. We are still a nation at war in Afghanistan. We still face threats to our homeland from terrorism."

—Secretary of Defense Leon Panetta, House Armed Services Committee Hearing on FY2013 Defense Budget.

January 2012

"As U.S. forces draw down in Afghanistan, our global counterterrorism efforts will become more widely distributed and will be characterized by a mix of direct action and security force assistance. Reflecting lessons learned of the past decade, we will continue to build and sustain tailored capabilities appropriate for counterterrorism and irregular warfare. We will also remain vigilant to threats posed by other designated terrorist organizations, such as Hezbollah."

—Sustaining U.S. Global Leadership: Priorities for 21st Century Defense, *Defense Strategic Guidance*, January 2012.

Guardian readers,

In the antiterrorism community, the terrorism landscape has changed significantly throughout the years. We've witnessed the 1983 bombing of the Marine Barracks in Beirut, the bombing of the Khobar Towers in 1998, the attack on the USS COLE (DDG 57), the events of 11 September 2001, and the killing of Osama bin Laden in 2011. We have faced terrorist threats throughout the world—from Afghanistan and Iraq to Yemen and North Africa to the Philippines and within the United States. The nature of terrorism—"the unlawful use of violence or threat of violence to instill fear and coerce governments or societies "—has not changed. However, the character of terrorism has changed. Throughout the years, the threat has evolved from hierarchical organizations, including state sponsors of terrorism targeting U.S. Servicemen overseas to a networked group of global jihadists attacking symbolic targets in the homeland to lone terrorists self-radicalized over the Internet acting alone within the heartland.

Throughout the history of *The Guardian*, we have explored a diverse range of topics. We have shared lessons learned, examined new technological initiatives, reviewed consequence management and preparedness, and placed terrorism within historical context.

In this vein, this issue of *The Guardian Antiterrorism Journal* explores issues that continue to challenge the AT/FP community.

- In **Selecting Security Countermeasures: Air Force Risk Management Decision Support with ForcePRO**, the author details an Air Force decision support tool that can aid commanders in determining the optimal allocation of resources through its automated Integrated Defense Risk Management Process.
- In **eGuardian: Threat and Suspicious Activity Reporting,** the writer discusses the Army's implementation of eGuardian, a sensitive but unclassified reporting system developed by the Federal Bureau of Investigation for suspicious activity reporting.
- **Freight Rail: Identifying and Defending Against the Unknown, Mile-long, 12,000-Ton Hazard** discusses the hazards and risks of freight rail near military installations and considerations when developing a rail emergency response plan.
- This issue also reflects on the Army's **Antiterrorism Doctrine FM 3-37.2** a year since its publication.
- **Fallacy of Security** challenges the conventional wisdom of AT efforts and offers some thoughts not just on terror protection but also on terror prevention.

This will be the final issue of *The Guardian*. Initially conceived in 2000 as a newsletter and formally published as a journal in 2003, *The Guardian* endeavored to create a forum for AT professionals across the Services to share thoughts and best practices in antiterrorism. *The Guardian* was relevant during the nascent stages of AT; it had value to those who were new in the career field, and it was particularly relevant when the field was growing. AT programs today are well established and subject matter expertise is resident at all levels of DoD. *The Guardian* served its intended purpose.

To our ardent readers and those who contributed articles, I thank you for your untiring support. Our commitment to the antiterrorism program remains strong, and we will continue to enlist your support for future endeavors. We will continue to think about how best to set the conditions for AT and to share our thoughts, ideas, and best practices across the Services and among the combatant commands, agencies, and field activities.

All the best,

JEFF W. MATHIS
MG, USA
Deputy Director for Antiterrorism/Homeland Defense

1 Joint Publication 3-07.2 "Antiterrorism." 24 November 2010, p. GL-7.

Selecting Security Countermeasures

U.S. Air Force photo by Airman 1st Class Brett Clashman/Released

Air Force Risk Management Decision Support with ForcePRO

By Larry Turner and Associates, Analytic Services Inc.

A complex security environment requires improved decision support tools.

America's geographic combatant commanders, as well as commanders of military installations worldwide, wrestle with common security concerns. These include maintaining a security posture to counter threats while implementing this posture with today's ever-tightening defense budget. Commanders need to have the best information available to make informed decisions on allocating limited security and defense resources. This information is vital, as commanders need to be able to implement the best security and defensive countermeasures possible, that is, those designed specifically to mitigate the risks from anticipated or known threats to critical assets. In times of plentiful resources, each security threat can be countered by implementing specific countermeasures. In these lean budget times, how can commanders determine and, more importantly, measure and validate which security countermeasures are the most important to implement?

These concerns are difficult to address. Many factors affect their resolution. Commanders operate in a difficult and complex security environment, regardless of where they are stationed or deployed and regardless of peacetime, crises, or actual war. Many threats, both external and internal to the department, must be considered; they include foreign military powers, nongovernment actors, and insider threats. Threats are constantly evolving and adapting at an increasingly quick rate compared to the security and defensive countermeasures used to combat them.

Many threats, both external and internal to the department, must be considered; they include foreign military powers, nongovernment actors, and insider threats. Threats are constantly evolving and adapting at an increasingly quick rate compared to the security and defensive countermeasures used to combat them.

Recognizing today's complex security environment, DoD is moving away from a checklist compliance security posture to one of risk mitigation; this requires a fundamental shift in the way commanders plan, resource, and implement their security and defensive countermeasures. This article describes how the U.S. Air Force Security Forces use ForcePRO software as the certified risk management decision support tool. ForcePRO automates the Integrated Defense Risk Management Process (IDRMP) and assists commanders in developing Integrated Defense Plans (IDP) focused on mitigating unacceptable risks. As described in Attachment 12 to Air Force Instruction 31-101, "Integrated Defense," ForcePRO was created by the Air Force Research Laboratory after subject matter experts conducted detailed security assessments at numerous Air Mobility Command and U.S. Air Forces in Europe installations.[1]

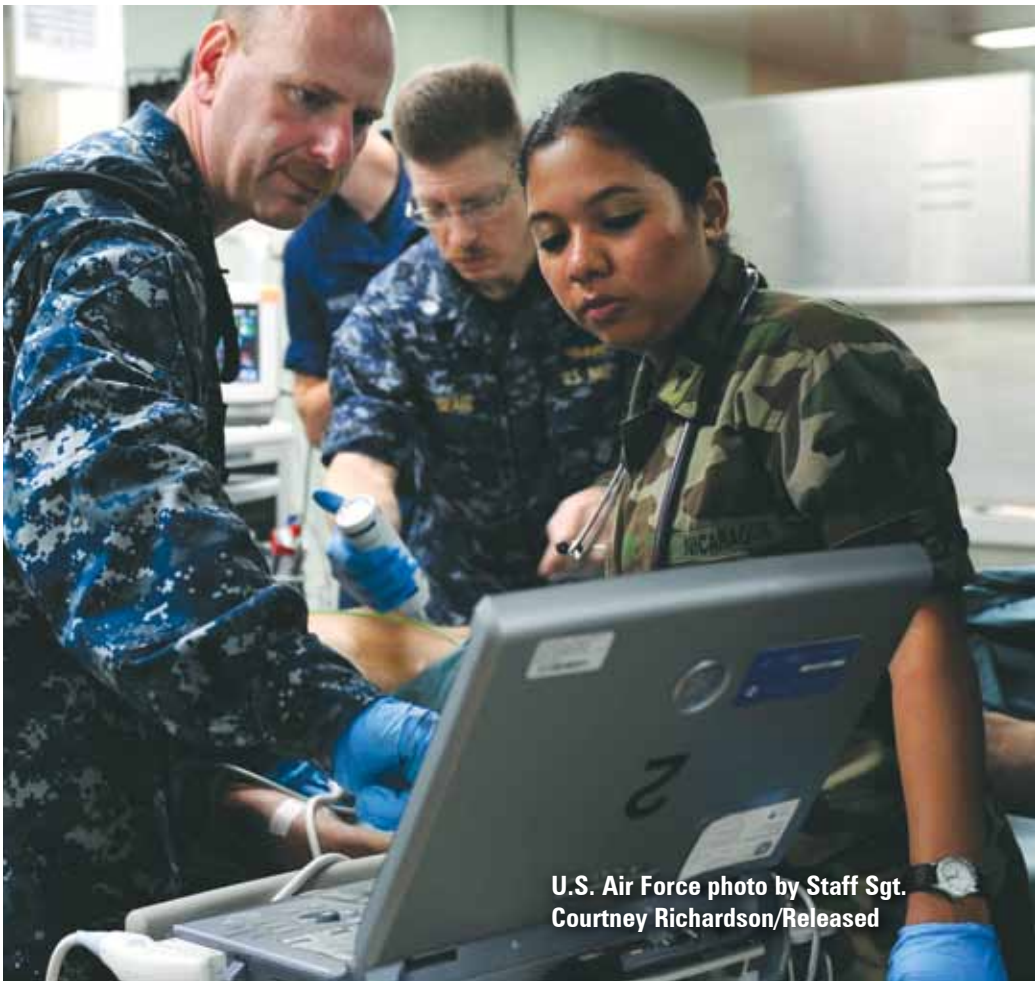
ForcePRO functions as a decision support tool by calculating the risks to specific critical assets on each installation. ForcePRO uses data input based on the commander's guidance as well as that of the Integrated Defense Council (IDC) and its Integrated Defense Working Group (IDWG) on asset criticality, asset vulnerability, and the threat. ForcePRO's benefits for the decisionmaking process include relieving risk management analysts from having to make the many repetitious, manual calculations necessary to determine risks to critical assets. In addition, through its risk calculations, ForcePRO highlights where the risks to critical assets are highest. Using this detailed information, commanders can then select specific security or defensive countermeasures to mitigate the risks. In this way, ForcePRO helps validate whether commanders are allocating resources in the best manner. ForcePRO's automation allows the IDWG to model numerous potential risk-reduction strategies and arrive at an acceptable revised risk.

ForcePRO's benefits for the decisionmaking process include relieving risk management analysts from having to make the many repetitious, manual calculations necessary to determine risks to critical assets.

A Change in the Way Commanders Implement Security Posture

Until recently, commanders implemented security postures through a lengthy set of compliance checklists full of detailed tasks. Security postures were assessed based on how well commanders complied with these checklists. The checklists were developed from a common set of vulnerability assessments that looked for the same types of threats worldwide. This situation required commanders to commit valuable resources to execute security or defensive countermeasures that were not necessarily based on addressing the current perceived, anticipated, or actual threats and did not consider the specific critical assets within these commanders' areas of responsibility. Today, the emphasis is on executing security management using risk management techniques. Risk management permits commanders to use the concept of Design Basis Threat (DBT) in developing

Today, DoD specifies that security plans must integrate multiple security functions and incorporate risk management.



U.S. Air Force photo by Staff Sgt. Courtney Richardson/Released

U.S. Air Force photo by Master Sgt. Trish Bunting/Released

Through its risk calculations, ForcePRO highlights where the risks to critical assets are highest. Using this detailed information, commanders can then select specific security or defensive countermeasures to mitigate the risks. In this way, ForcePRO helps validate whether commanders are allocating resources in the best manner.

security and defensive plans and in formulating risk tolerance. DBT, as defined in Joint Publication 3-07.2, "Antiterrorism," is the threat against which an asset must be protected and on which the protective system's design is based.[2] DBT permits commanders to tailor their security and defensive countermeasures to the known or anticipated threats against their specific installations and critical assets.

Today, DoD specifies that security plans must integrate multiple security functions and incorporate risk management. DoD Directive (DoDD) 2000.12 specifies that the DoD "AT Program shall be all encompassing" and shall use "an integrated systems approach."[3] In addition, this AT capstone policy directs the DoD AT Program to incorporate the critical elements of "AT risk management, planning, training and exercises, resource generation, and a program review." The DoD Physical Security Program, as prescribed in DoDD 5200.28-R, echoes this risk management philosophy, stating that all security functions should be coordinated in support of an integrated and coherent effort.[4] This effort includes operations security, law enforcement, information security, personnel security, communications security, automated information security, counterintelligence, and AT programs.

This policy means that commanders responsible for implementing security programs must take a holistic view of the security environment. They must evaluate the

known and anticipated threats to the critical assets within their areas of responsibility, assess the vulnerability of these critical assets to the known and anticipated threats, and then decide which countermeasures are the best for mitigating the risks. When long-term employment of security countermeasures is impracticable due to sustainment costs, commanders may direct an evaluation of the installation's security posture to determine suitable mitigation options to counter risk above the commander's risk-tolerance threshold.

The U.S. Air Force Integrated Defense Risk Management Process

The U.S. Air Force has implemented installation defense and security risk management through its IDRMP and has published Air Force Instruction 31-101, "Integrated Defense," to govern its implementation Servicewide. Air Force Security Forces risk management analysts enter critical asset information, vulnerabilities, and threat data into the ForcePRO application to support their commanders' critical security decisions. A significant benefit of ForcePRO is that it can be used by all military organizations worldwide. Installations that have common missions, that operate in similar environments, or that face similar threats can share their ForcePRO data to identify common risks and provide their commanders with additional information to base decisions on when selecting security or defensive countermeasures (see Figure 1).

Installations that have common missions, that operate in similar environments, or that face similar threats can share their ForcePRO data.

Figure 1. Sharing ForcePRO information[5]

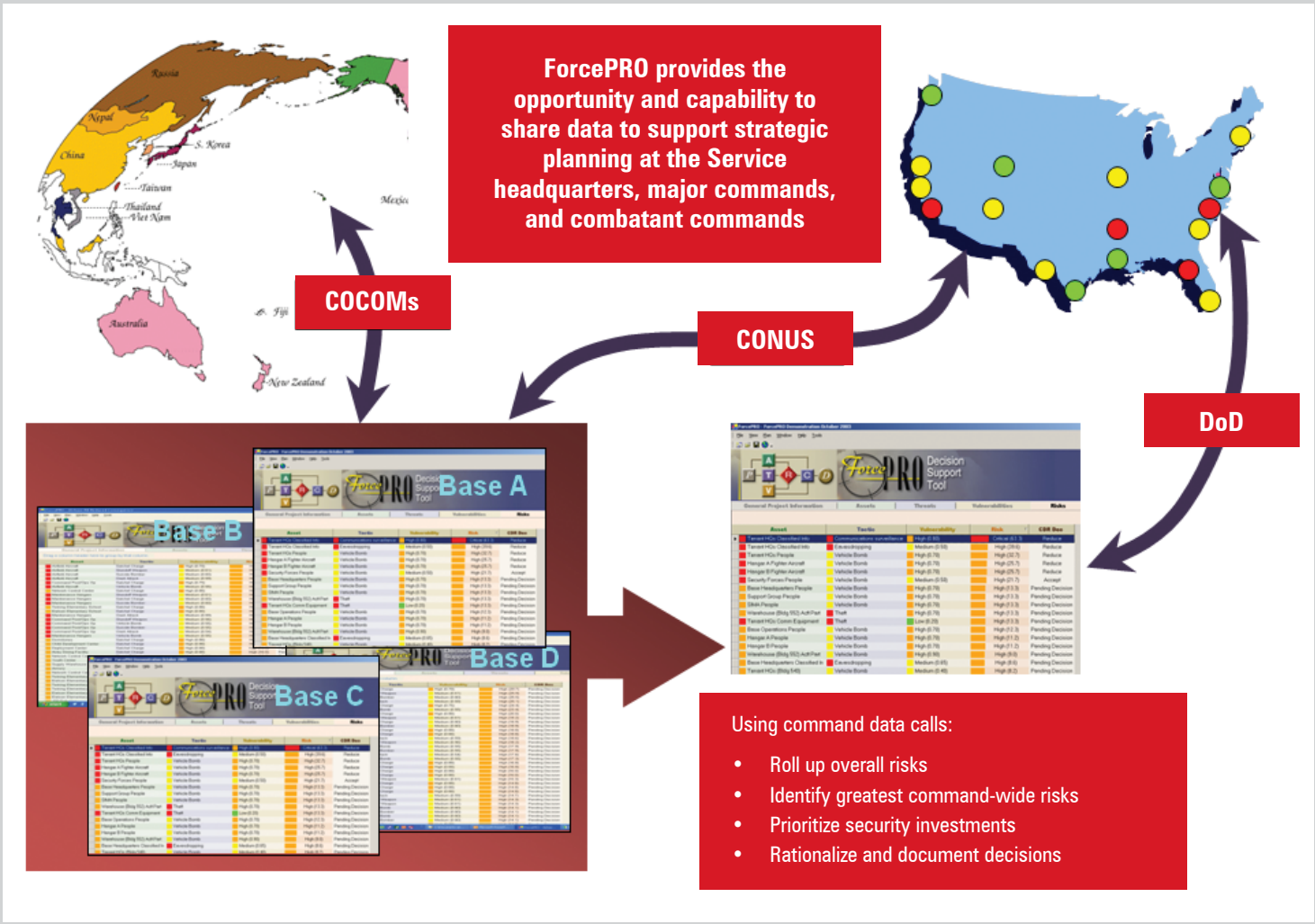


Figure 2. ForcePRO Critical Asset Risk Rating Scale[5]

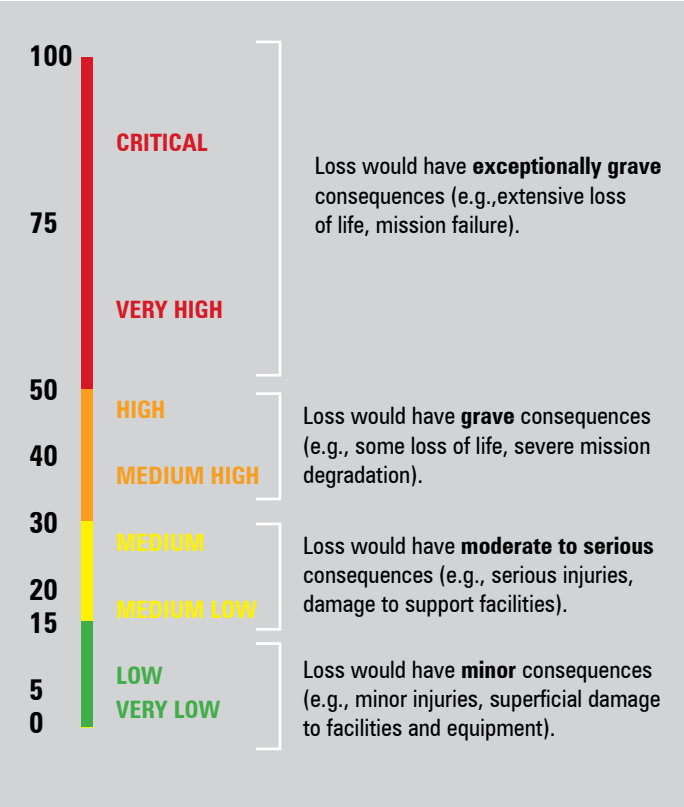
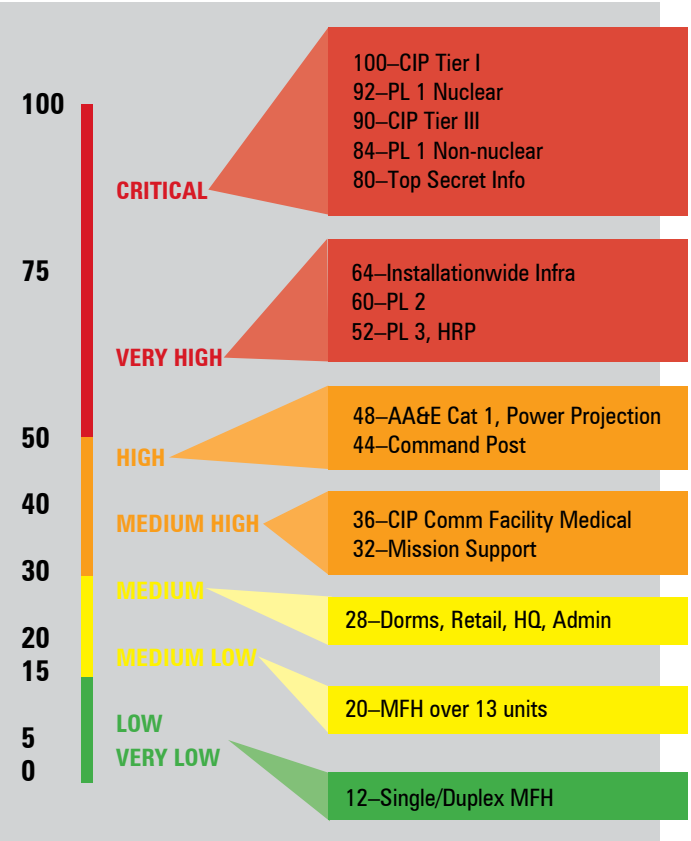


Figure 3. ForcePRO Prescored Critical Asset Risk Rating Scale[5]



Linking Risk Management to Security Planning

To fully incorporate the value-adding benefits of risk management into security planning, commanders need an efficient and comprehensive decision-support tool to help them calculate risk, develop their risk-tolerance decisions, and select the countermeasures that best mitigate risks. The IDC serves as a commander's principal staff element responsible for oversight and coordination of the IDRMP and subsequent development of the IDP. The IDC's working group, the IDWG, uses ForcePRO to calculate the criticality of assets, to assess the threat level, and to identify the vulnerability of the critical assets on the installation.

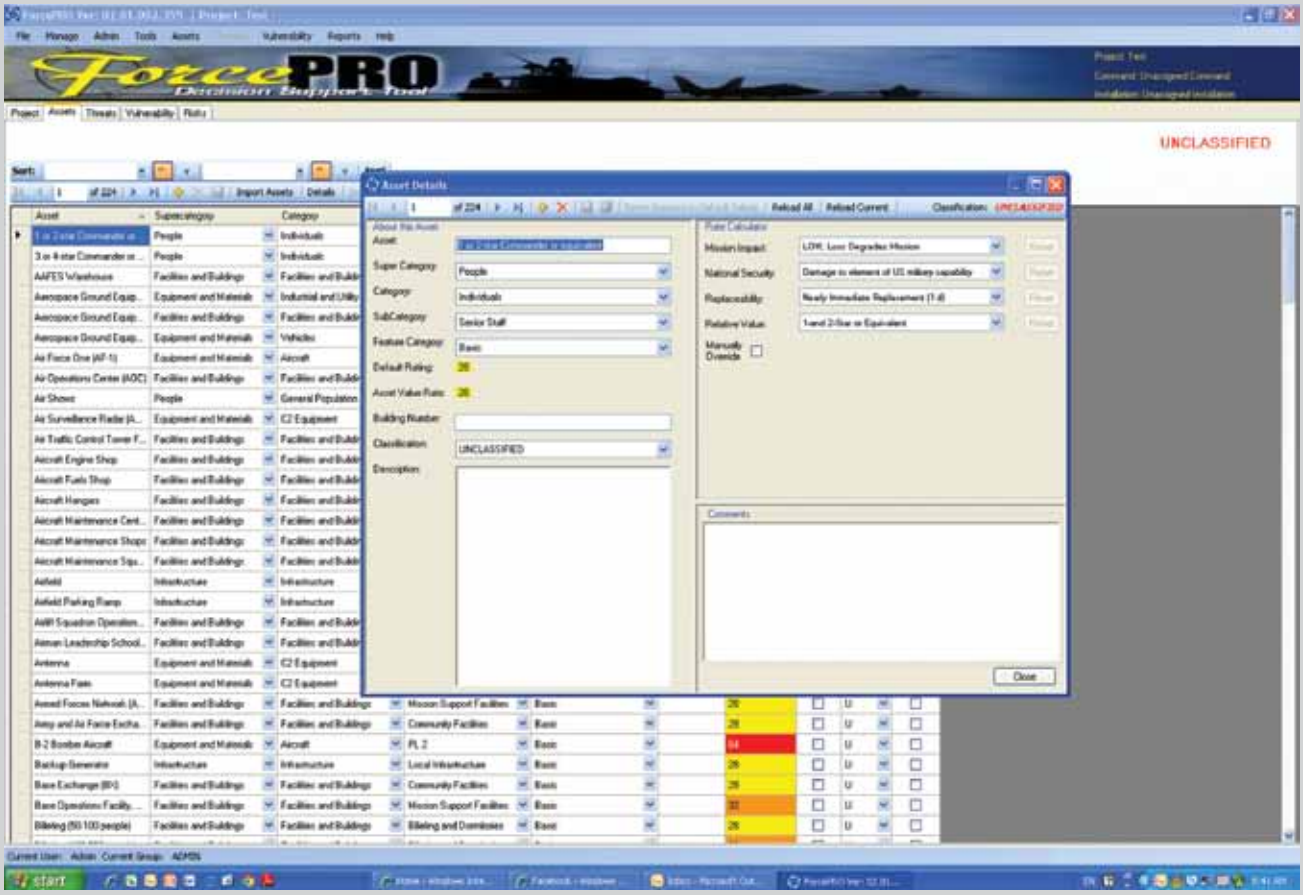
The IDWG identifies threats through the intelligence preparation of the battlespace/battlefield and integrates the commander's guidance with the mission statements for the installation's organizations to develop critical asset lists. These assets are then matched to vulnerabilities in the context of how vulnerable these assets are to the anticipated or known threats. Using scales, as in the example in Figure 2, working groups enter a numerical value for asset criticality and vulnerability into the ForcePRO application, which subsequently calculates the criticality of the highest-priority assets on each installation and their vulnerability based on current actual and anticipated threat assessments.

ForcePRO offers Critical Asset and Risk Rating Scales based on 100 points to permit working groups to identify and assign the recommended appropriate score for each scale. ForcePRO has prescored lists (Figure 3) and asset detail screens (Figure 4) in which risk management analysts (e.g., the Defense Force Commander) can enter specific details of each critical asset to assist in determining appropriate ratings. After thoroughly analyzing the critical assets, their vulnerabilities, and the threat, these specific values can be entered into the ForcePRO database. Note that ForcePRO assigns each critical asset a default, or prescored, rating. Risk management analysts can change this default rating by entering the specific details into the Rate Calculator drop-down menus on the right of the asset screen (see Figure 4).

ForcePRO then produces a Risk Summary Report (Figure 5) with asset, threat, and vulnerability ratings, plus an overall risk rating. Commanders can then use these ratings to develop their prioritized security and defensive countermeasures. The risk-summary report shows the unwanted event (loss of the function of a critical asset due to a threat tactic) and the criticality scores for each asset, together with their respective vulnerability and threat scores. After application of countermeasures, ForcePRO calculates the revised risk for all three elements of risk and the risk score based on the perceived effectiveness of the countermeasures.

These analytic processes, combined with ForcePRO's calculation abilities, allow the IDC and the IDWG to have

Figure 4. ForcePRO Asset Detail Screen[5]



a logical, well-structured discussion about mitigating the risks to their critical assets. At a certain point, these discussions will reach the stage where the IDC can offer the commander enough information with which to make a risk-tolerance decision, that is, whether to accept the risk or to direct courses of action to mitigate it. The commander may want all risk mitigated to a low rating;

ForcePRO, with its ability to calculate risk quickly using detailed asset criticality and vulnerability input from the IDC and working group analysts, can support this continuous assessment and help commanders determine the optimal allocation of resources to implement the best security and defensive countermeasures possible.

may consider a revised risk rating of 32 an acceptable score; or may limit countermeasures to existing security force tactics, techniques, and procedures to lower risk rather than invest resources in new countermeasures to lower the risk. After the commander makes the risk decision, it is time to develop courses of action for security and/or defensive countermeasures.

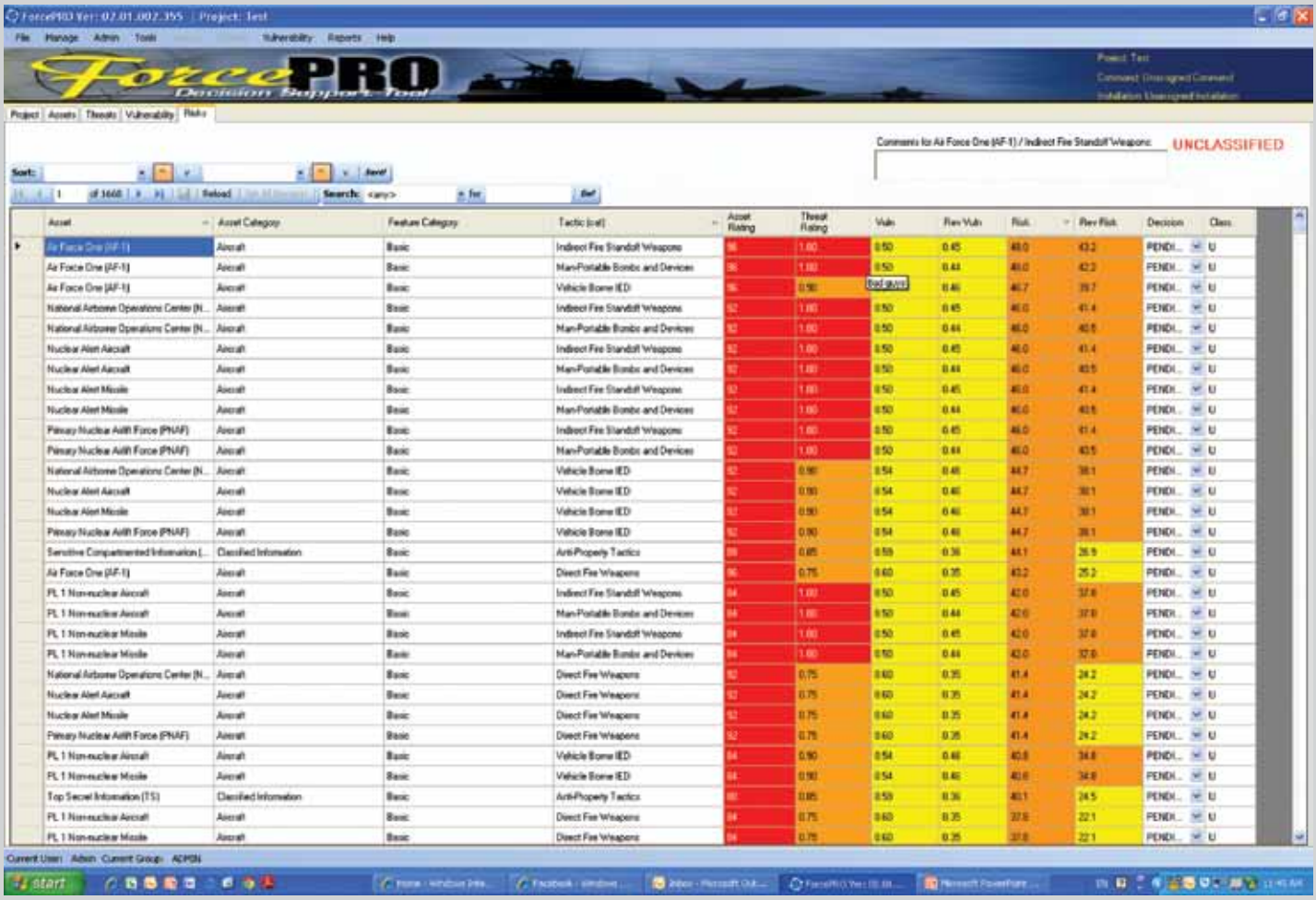
Incorporating ForcePRO into the IDRMP and Security Planning

Once the IDC receives the commander's intent and the commander's critical information requirements, the IDWG executes the IDRMP, cycling through the process of analyzing the installation defense mission and identifying the inherent specified and implied tasks. The IDRMP lists critical assets to protect, assesses the threat, assesses the vulnerability of critical assets, and finally, calculates the risk assessment using the following formula:

$$\underset{\text{assessment}}{\text{risk}} = \underset{\text{assessment}}{\text{criticality}} \times \left(\underset{\text{assessment}}{\text{threat}} \times \underset{\text{assessment}}{\text{vulnerability}} \right)$$

At the completion of these steps, the IDP can draft multiple courses of action to present to the installation commander, who will issue guidance and the risk-tolerance decision. This information is incorporated into the final IDP and presented to the commander for decision. It is important to understand that each course of action is part of the overall risk-reduction strategy

Figure 5. ForcePRO Risk Summary Report[5]



and may require full implementation or can be phased to match emergent threats seeking to exploit identified vulnerabilities. This factor is key to resolution of risk in a fiscally restrained environment but is very obtainable when the tools and the planning are matched to support a comprehensive integrated defense systems approach.

It is important to note that the final implemented IDP will have an impact (as it is designed to do) on the threat and quite possibly on the vulnerability of each asset. This impact will result in a revised risk and is why the IDRMP is a continuous cycle. The threat will react to the IDP implementation, and that reaction may require changes in security and defense countermeasures to keep the threat risk at the lowest possible level. ForcePRO, with its ability to calculate risk quickly using detailed asset criticality and vulnerability input from the IDC and working group analysts, can support this continuous assessment and help commanders at installations, major commands, and geographic combatant commands determine the optimal allocation of resources to implement the best security and defensive countermeasures possible.

If you have any questions regarding the Air Force IDRMP or ForcePRO, please contact Maj Greg Bodenstein, DSN: 945-5004, gregory.bodenstein@us.af.mil, at the HQ Air Force Security Forces Center, Integrated Defense Cell.

1 Air Force Instruction 31-101, "Integrated Defense," 8 October 2009; available for authorized users to download, or to order on the Warehouse Management System (WMS) at https://wmsweb.afncr.af.mil/wms/default.aspx

2 Joint Publication 3-07.2, "Antiterrorism," 24 November 2010; available through the Joint Doctrine Education and Training Electronic Information System (JDEIS).

3 DoDD 2000.12, "DoD Antiterrorism (AT) Program," 18 August 2003; available at http://www.dtic.mil/whs/directives/corres/dir.html

4 DoDD 5200.08-R, "Physical Security Program," 9 April 2007; available at http://www.dtic.mil/whs/directives/corres/pub1.html

5 Bowman, D., & Kinner, M. "IDRMP Overview Presentation." Undated. Available by permission from Analytic Services Inc.

6 DoD Instruction 2000.16, "DoD Antiterrorism (AT) Standards," 2 October 2006; available at http://www.dtic.mil/whs/directives/corres/ins1.html

(U.S. Air Force photo by Master Sgt. Shane A. Cuomo/Released)

eGUARDIAN

THREAT AND SUSPICIOUS ACTIVITY REPORTING

Applying Tactical Intelligence Doctrine To Antiterrorism

This article was written by staff from the Antiterrorism Branch, Office of the Provost Marshal General; Law Enforcement Branch, Office of the Provost Marshal General; and Criminal Investigation Division

Whether a plan for a terrorist attack is homegrown or originates overseas, important knowledge that may forewarn of a future attack may be derived from information gathered by state, local, and tribal government personnel in the course of routine law enforcement and other activities.

—National Strategy for Information Sharing, October 2007

DoD Instruction (DoDI) 2000.26, "Suspicious Activity Reporting" (1 November 2011), directs the DoD to utilize the eGuardian system as the authorized DoD law enforcement suspicious activity reporting (SAR) system. The eGuardian system is a sensitive but unclassified reporting system developed, owned, and operated by the FBI. It allows the FBI to collect suspicious activity (SA) threat information that has a potential link to terrorism and to share the information with other federal, state, local, and tribal law enforcement. It is restricted to law enforcement personnel and law enforcement analysts. The eGuardian system is accessible through a special interest group within the FBI's Law Enforcement Online (LEO) information system. The eGuardian system links

The eGuardian system plays a critical role in our ability to fight terrorists by gathering SA reporting and by assisting criminal intelligence analysts in its efforts to assess and warn the Army community of credible threats.

unclassified, For Official Use Only, and law enforcement–sensitive reporting information to the FBI's Guardian

Suspicious activity **is defined as observed behavior that may be indicative of intelligence gathering or other preoperational planning related to terrorist or other security threats to DoD interests worldwide.**

Program. Guardian is a web-based system on the classified FBI network that is designed to allow for the transmission of terrorist threat and SA information within the FBI.

In 2008, the FBI created eGuardian to report and share unclassified potential terrorist threats, events, and SA among local, state, tribal, and federal law enforcement agencies, fusion centers, and terrorism task forces. From an Army law enforcement or protection perspective, the purpose of eGuardian reporting is to assist commanders in determining the aggregate threat and to keep commanders at all levels informed of threat conditions. This allows commanders to initiate effective security responses and threat countermeasures.

The July 2011 attack in Norway highlights the need for 360° vigilance to identify potential threats inside and outside Army communities. The ability to detect, report, and deter threats is as important as our ability to respond.

To strengthen DoD efforts to counter terrorist threats, those responsible for protecting DoD resources must have timely access to properly acquired threat information, particularly information that indicates a potential threat from those who want to attack the United States. This includes information on terrorists' plans, capabilities, activities, and intended targets. The eGuardian system plays a critical role in our ability to fight terrorists by gathering SA reporting and by assisting criminal intelligence analysts in their efforts to assess and warn the Army community of credible threats.

Because eGuardian is a law enforcement SA reporting tool, the Office of the Provost Marshal General (OPMG) is responsible for management, oversight, and control of eGuardian within the Army. OPMG delegated program management of eGuardian (within the Army) to the U.S. Army Criminal Investigation Command (USACIDC). The Army's military intelligence community and Army subordinate commands (down to installation, stand-alone facility, and unit level) share the responsibility for establishing education and reporting procedures that contribute to the timeliness and quality of SA reporting. Within the Army Protection Program, threat working groups at all levels must work closely with the supporting USACIDC office, the provost marshal (PM), or the director of emergency services (DES) to establish a system for receiving timely threat information. The developed information assists commanders in making decisions regarding threat information dissemination, changes to FP conditions, and execution of random AT measures.

As the Army's program manager, USACIDC serves as the access manager for all authorized personnel and entities within the Army with the exception of the National Guard (managed by National Guard Bureau PM). Access to the eGuardian system is via the FBI's LEO system. DoD personnel whose law enforcement responsibilities require access to the eGuardian system

U.S. Army photo by Spc. Venessa Hernandez/Released

Although the eGuardian system is in the early stage of Armywide implementation, enhanced education and awareness of SA and the eGuardian system have led to an increase in SA reporting. SA awareness campaigns and education of Army leaders at all levels will increase SA reporting. Within the CID, PM, and DES community, leaders are actively expanding the number of eGuardian users. The end result of increased awareness and reporting will be greater situational awareness. (U.S. Navy photo by Gary Nichols/Released)

must establish LEO accounts by applying directly to the FBI for access via the LEO website (www.leo.gov). The eGuardian access procedures can be found in the *eGuardian Information and Users Guide*. Four distinct types of eGuardian accounts are approved for use by DoD personnel: user, supervisor, approver, and read-only. The USACIDC is responsible for ensuring processing, validation, and approval of requests for eGuardian access as well as management of user accounts.

The iWATCH Army Program provides useful information to educate the Army community about the indicators of SA and to encourage citizens, dependents, and Soldiers to report suspicious activities or behaviors to military police or local law enforcement for investigation. To protect law enforcement–sensitive information, only DoD law enforcement personnel and analysts assigned to law enforcement activities will enter SAR data into eGuardian.

Reportable information received by law enforcement agencies is reviewed and analyzed at all levels to identify current threats, emerging trends, and future indicators. The DoD established 13 categories of actions and behaviors that merit reporting via the eGuardian system (available in the *eGuardian Information and Users Guide*).

The DoD established 13 categories of actions and behaviors that merit reporting via the eGuardian system. Although some reports may not have a clear nexus with terrorism, the indicators can be used for pattern and trend analysis and retained for 5 years.

Although some reports may not have a clear nexus with terrorism, the indicators can be used for pattern and trend analysis and retained for 5 years. Incidents determined to have "no link to terrorism" are removed

from the eGuardian system within 180 days of the final determination.

Criminal intelligence products developed and disseminated based on analysis and collaborative efforts between USACIDC and Army intelligence are listed below. These products include input from external entities, such as the Counterintelligence Law Enforcement Cell (CILEC), the Antiterrorism Operations and Intelligence Cell (ATOIC), the FBI, Joint Terrorism Task Forces (JTTF), the Naval Criminal Investigative Service (NCIS), the Air Force Office of Special Investigations (AFOSI), other federal agencies, state fusion centers, and other law enforcement partners:

- Daily Terrorism Summary (CIOC)
- Military Intelligence and Law Enforcement Summary
- USACIDC Suspicious Activity Reporting–Summary (SAR-S)

Although the eGuardian system is in the early stage of Armywide implementation, enhanced education and awareness of SA and the eGuardian system have led to an increase in SA reporting. SA awareness campaigns and education of Army leaders at all levels will increase SA reporting. Within the Criminal Investigation Department (CID), PM, and DES community, leaders are actively expanding the number of eGuardian users. The end result of increased awareness and reporting will be greater situational awareness.

An *eGuardian Information and Users Guide,* information poster, and SA reportable categories pocket card are available on the Army's Antiterrorism Enterprise Portal (ATEP) for download and distribution locally (https://www.us.army.mil/suite/page/605757).

Upcoming AT Seminars, Conferences, & Training

SERVICE	CONFERENCE	LOCATION	DATE
Navy	OPNAV AT Conference	Pentagon	May 2012
Joint Staff	J-34 Joint Staff Level IV AT Executive Seminar	McLean, VA	8–10 May 2012
Army Office of the Provost Marshal General	MP and CID Senior Leaders' Conference	Leesburg, VA	7–11 May 2012
USAFRICOM	USAFRICOM Antiterrorism Conference	Garmisch, Germany	11–15 June 2012
USSOCOM	USSOCOM AT Conference	Tampa, FL	19–21 June 2012
DoD	Antiterrorism Vulnerability Assessment Benchmark Workshop	Chantilly, VA	10–12 October 2012
Joint Staff	J-34 Joint Staff Level IV AT Executive Seminar	McLean, VA	23–25 October 2012
Army	Worldwide AT Conference	Orlando, FL (Shades of Green)	January/February 2013 (TBD)

TRISA WOT Poster No. 03-12
U.S. Army TRADOC G2 Intelligence Support Activity
(*Source:* DOD Defense Imagery: U.S. Army Photo)

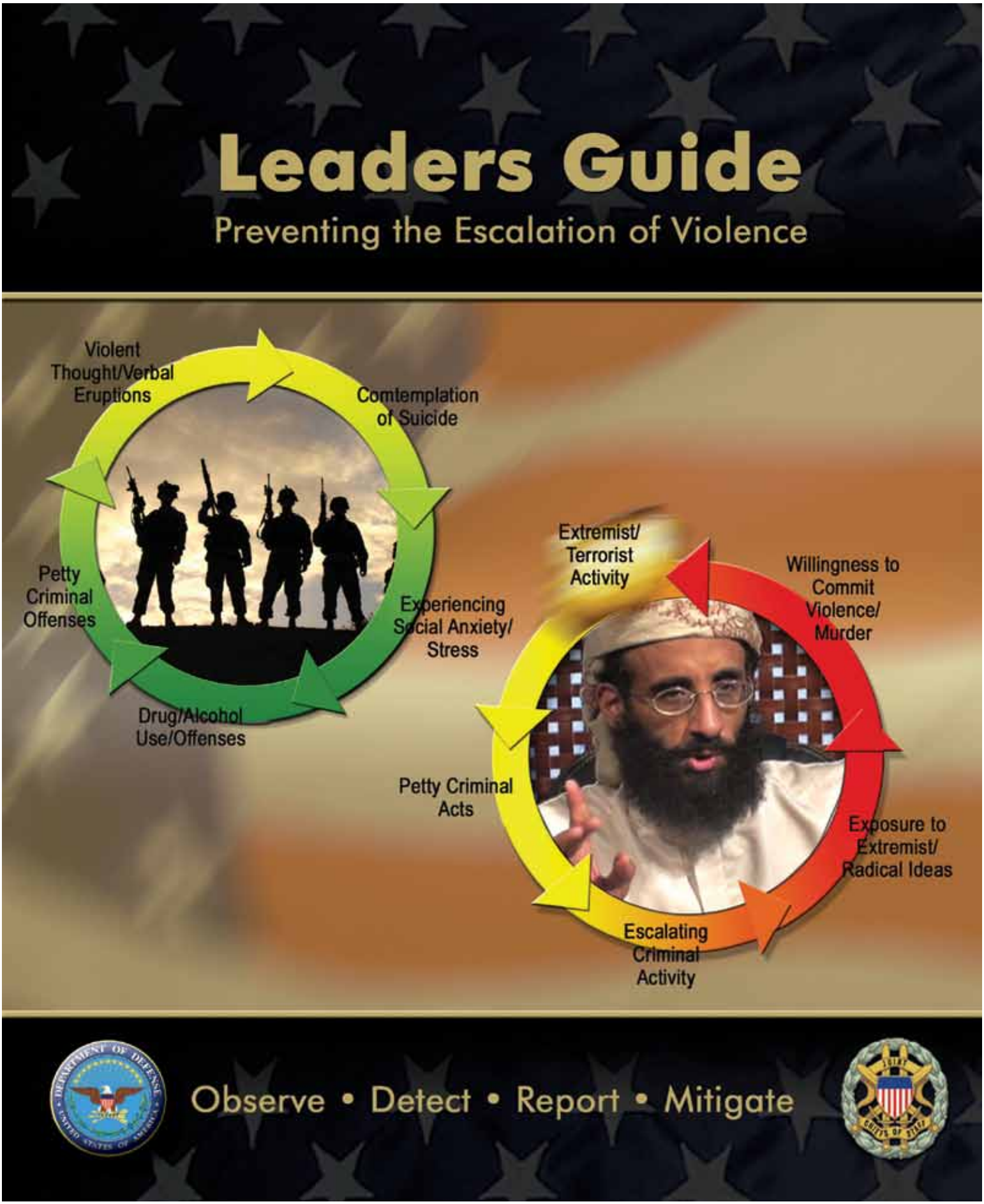
Indicators of Potential Terrorist Associated Insider Threat

- Advocating support for terrorist organizations or objectives.
- Expressing hatred of American society, culture or government, or principles of the U.S. Constitution.
- Advocating the use of violence to achieve political, religious, or ideological goals.
- Sending large amounts of money to persons or financial institutions in foreign countries.
- Expressing a duty to engage in violence against DoD or the United States.
- Purchasing bomb-making materials.
- Inquiry or obtaining information about the construction and use of explosive devices.
- Expressing support for persons or organizations that promote or threaten the unlawful use of violence.
- Advocating loyalty to a foreign interest over loyalty to the United States.
- Financial contribution to a foreign charity or cause linked to an international terrorist organization.
- Evidence of terrorist training or attendance at terrorist training facilities.
- Repeated viewing of Internet Web sites, without official sanction, that promote or support international terrorist themes.
- Posting comments or exchanging information, without official sanction, at Internet chat rooms, message boards, or blogs that promote the use of force directed against the United States.
- Joking or bragging about working for a foreign intelligence service or associating with international terrorist activities.

Report Suspicious Activity:

- Contact your local Counterintelligence (CI) office
- CONUS Hotline: 1 – 800 – CALL SPY (1–800–225–5779)
- iSALUTE – The CI reporting portal via AKO at: https://www.us.army.mil/suite/page/633775
- iWATCH ARMY – https://www.us.army.mil/suite/page/605757

U.S. ARMY ARMY STRONG®



See poster insert on page 19 for details.

LEADERS GUIDE

Preventing the Escalation of Violence

OBSERVE • DETECT • REPORT • MITIGATE

Recognizing Signs of High-Risk Behavior

Indicators of high-risk behavior may include the following:

- Lack of positive identification within community
- Involvement across the violence spectrum
- Participation in lower-impact criminal activity or rule-breaking
- Increased use of alcohol or drugs
- Diagnosis of a mental health disorder, including depression
- Increased severe mood swings and noticeably unstable or emotional responses
- Increase in unsolicited comments about violence, firearms, and other dangerous weapons or violent crimes
- Defense of extremist or radicalized views
- Unusual accumulation of weapons, training manuals or other dangerous supplies

When indicators of potential violent behavior overlap with indicators of suicidal tendency, a synergistic effort between these elements should lead to information sharing, cross-talk, and standardized processes to aid in identifying personnel who may present an insider threat or have a potential for terrorist-related activity.

Personnel who are identified within this realm warrant further investigation by leadership and possibly law enforcement.

Monitoring Behavior

Commanders are empowered with numerous tools and authorities to take steps to promote the general welfare of Soldiers under their command. Examples:

- Organizational Inspection Programs
- Health and Welfare Inspections
- Urinalysis
- Privately Owned Weapon Registration
- Individuals participating in medical treatment programs and services, such as drug abuse prevention, family advocacy, and behavioral health programs, should also be screened for violent and extremist behavior, including a propensity toward violent and extremist activity

Preventing the Worst

Preventing insider threats or terrorist attacks involves much more than physical security measures. Recognizing indicators of high-risk behavior (such as criminal activity or associating with violent groups) that may lead to an escalation of violence, and addressing those issues, may reduce the potential for violent acts committed against the community.

Unit leaders, medical service providers, and the protection community must communicate effectively to develop a complete and accurate picture of an individual's propensity for future violence.

- Antiterrorism & Protection Professionals

- Unusual, unexplained selling or giving away of personal possessions

Unity of Effort

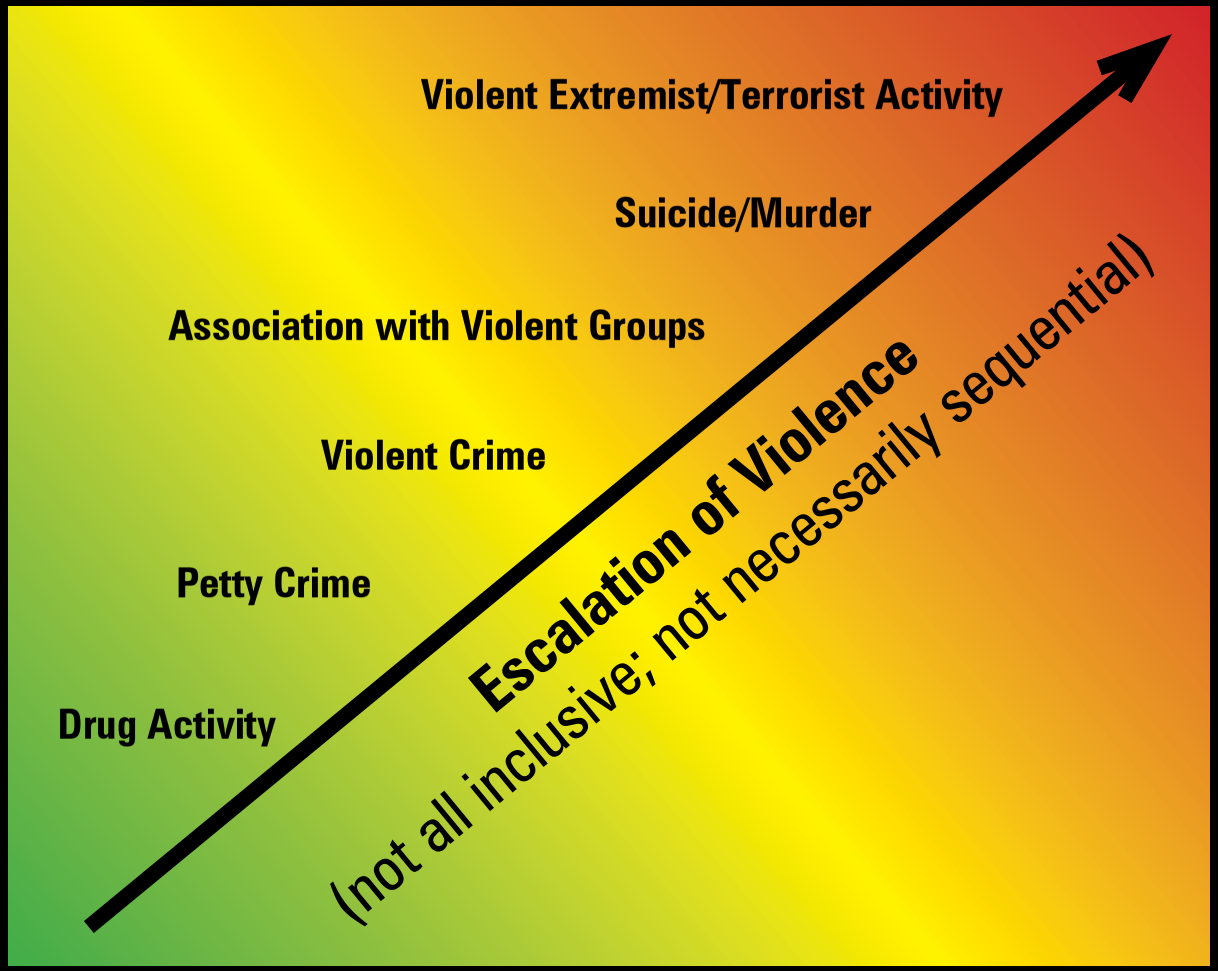
By approaching violence prevention comprehensively, medical service providers, supervisors/leaders, and protection personnel can work together to detect indicators of possible future violent or extreme behavior.

- Commander's Disciplinary Action
- Commander's Risk Indicator Dashboard
- Family Readiness and Feedback

Detection of high-risk behavior requires a multidisciplinary approach. Administrative tools that commanders use to improve unit readiness may have a secondary and positive risk reduction benefit to help counter insider threat or terrorist activity.

- Law Enforcement
- Medical Providers
- Commanders and Leaders (particularly first line supervisors)
- Soldiers and Civilians.

The Violence Spectrum



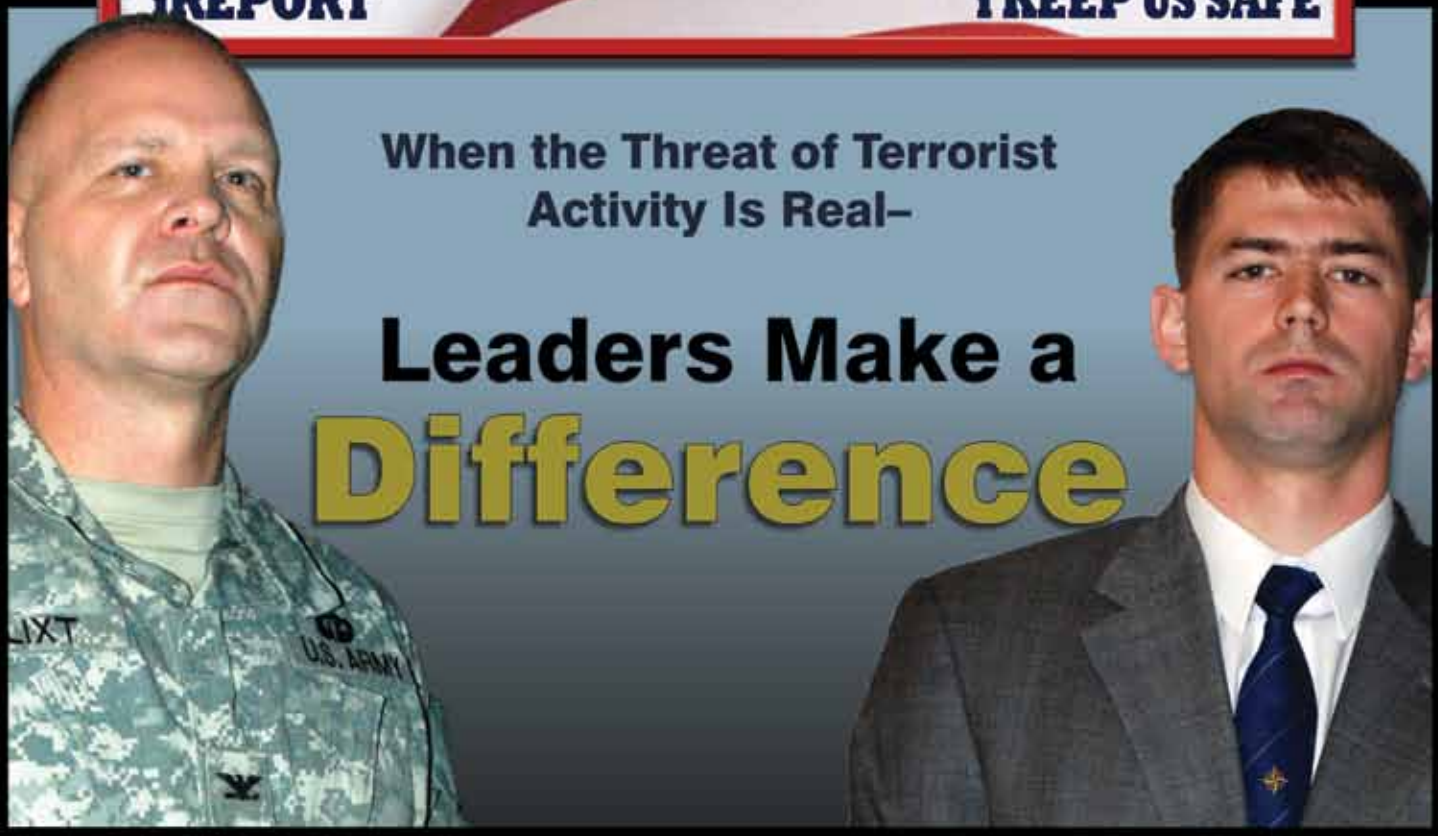
By mitigating lower-impact, higher-frequency violence (particularly high-impact criminal acts) leaders may be able to prevent an escalation of violence.

- Small-scale violence or antisocial behavior (such as simple assault, harming animals) may indicate a propensity for violence.
- Individuals who defend violent extremism, regardless of political or religious affiliation, should be monitored closely.
- High-risk indicators overlap, and the potential effects of those behaviors should not be treated in isolation (e.g., suicidal tendencies could lead to an active shooter situation, individuals exhibiting high-risk behavior may be vulnerable to extremist/terrorist group radicalization).
- Health promotion/risk reduction monitoring and treatment programs may help detect indicators and reduce possibilities of violence.

iWATCH

iREPORT

i KEEP US SAFE



When the Threat of Terrorist Activity Is Real–

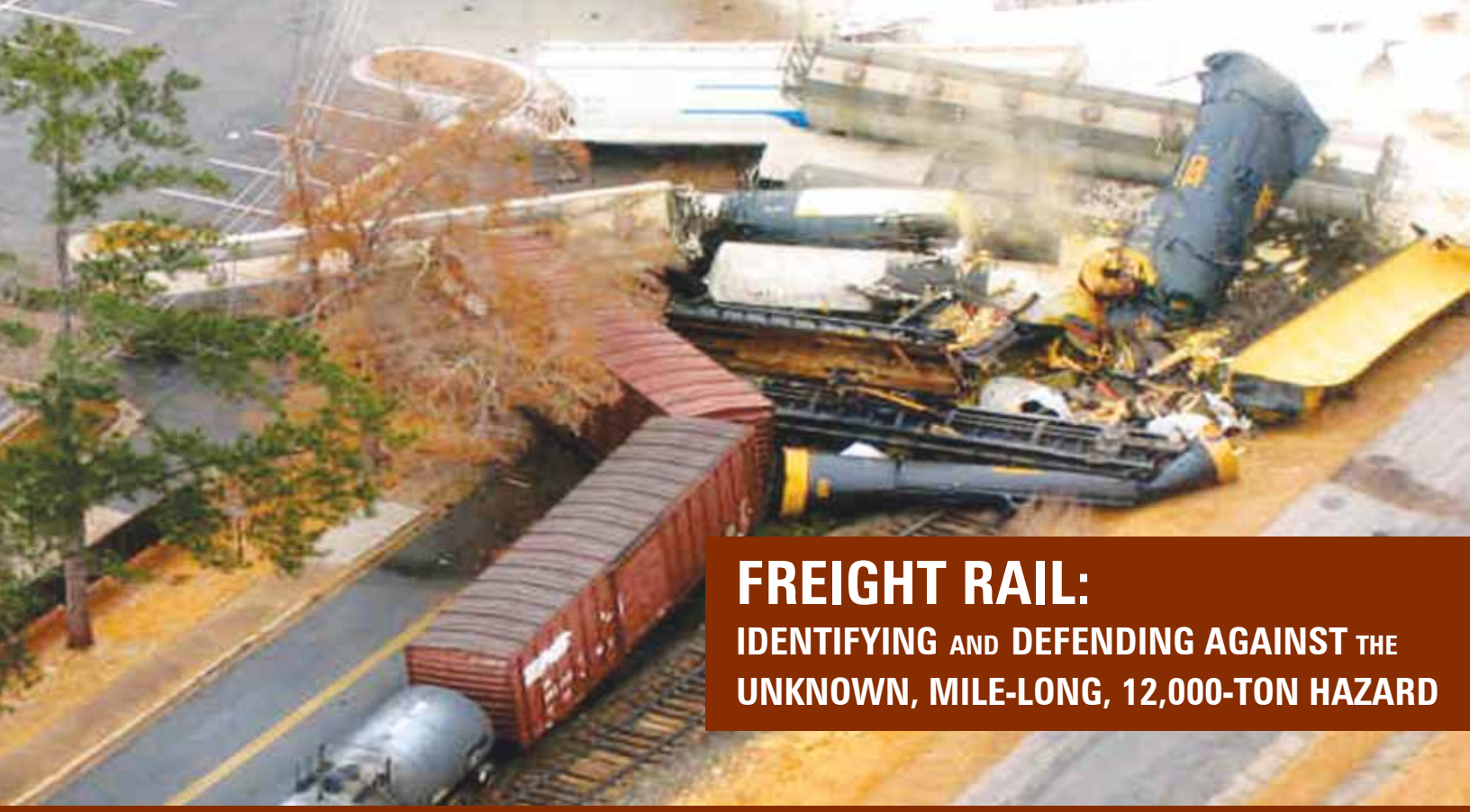
Leaders Make a Difference

Leaders, do you know:

- Your role and responsibility?
- Your unit's responsibility?
- What to tell your soldiers, DoD civilians and families?
- What individuals can do to prevent terrorist acts?
- How to report suspicious activity or behavior?
- The indicators of high-risk behavior?
- Where you can find antiterrorism information?

Always Ready, Always Alert

Because someone is depending on you



FREIGHT RAIL:
IDENTIFYING AND DEFENDING AGAINST THE UNKNOWN, MILE-LONG, 12,000-TON HAZARD

Emergency planning and hazard assessments for railroad disasters

By Robert C. Massey, Defense Threat Reduction Agency (DTRA) Joint Staff Vulnerability Assessment Team 4

Release of HAZMAT from a railroad incident, whether the result of attack or accident, could adversely affect an installation's critical facilities, mission, personnel, and assets.

Does Your Installation Properly Plan for Nearby Rail Systems?

Do you know what is being transported near your installation? Are your first responders properly equipped and trained to respond to a railroad incident involving thousands of pounds of hazardous material (HAZMAT)? Does your emergency plan outline response capabilities and procedures to address a railroad incident? If you answered no to any of these questions, then your installation likely needs to review its hazard assessment and revise its emergency plans.

What Hazards and Risks Are Associated with Railroad Operations Near Military Installations?

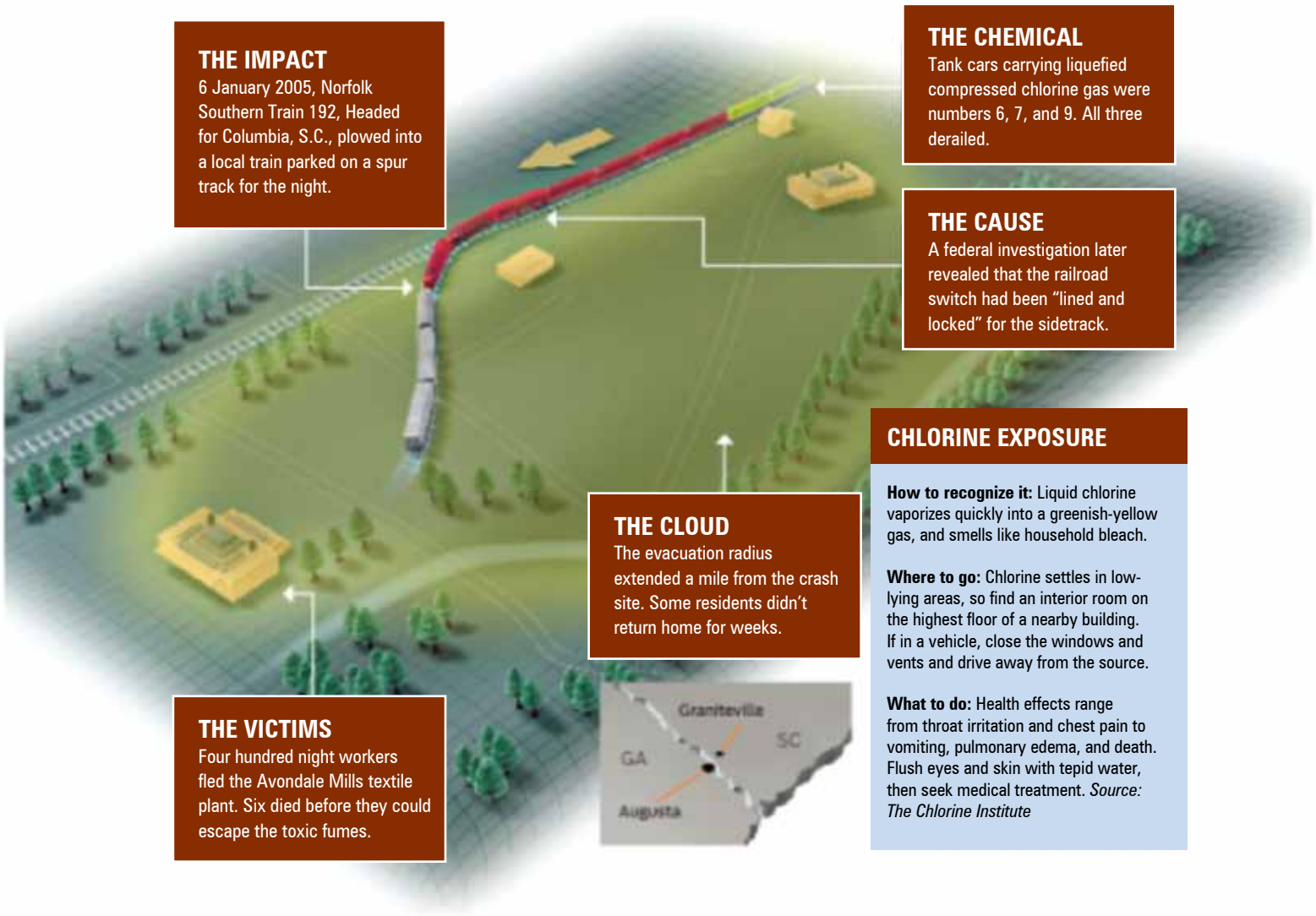
Each day, Americans use millions of commercial products—everything from food packaging to electronics—formulated using raw materials and chemicals that can be hazardous if released during transport. This HAZMAT is often transported in close proximity to our military installations and, in the event of a release, could unleash the same destruction and consequences as a weapon of mass destruction.

According to the Association of American Railroads Bureau of Explosives, each year more than 76,000 bulk rail shipments of materials that are poisonous by inhalation, commonly referred to as toxic inhalation hazard (TIH), traverse nearly all major American cities and metropolitan regions.[1] Rail accidents for 2010 totaled

Hazardous materials are often transported in close proximity to our military installations and, in the event of a release, could unleash the same destruction and consequences as a weapon of mass destruction.

1,830, which included 732 fatalities and 4,272 nonfatal employee injuries, according to the Federal Railroad Administration 2010 safety results.[2]

Release of HAZMAT from a railroad incident, whether the result of attack or accident, could adversely affect an installation's critical facilities, mission, personnel, and assets.



The Vulnerability of Industrial Railroads Makes Them an Attractive Target

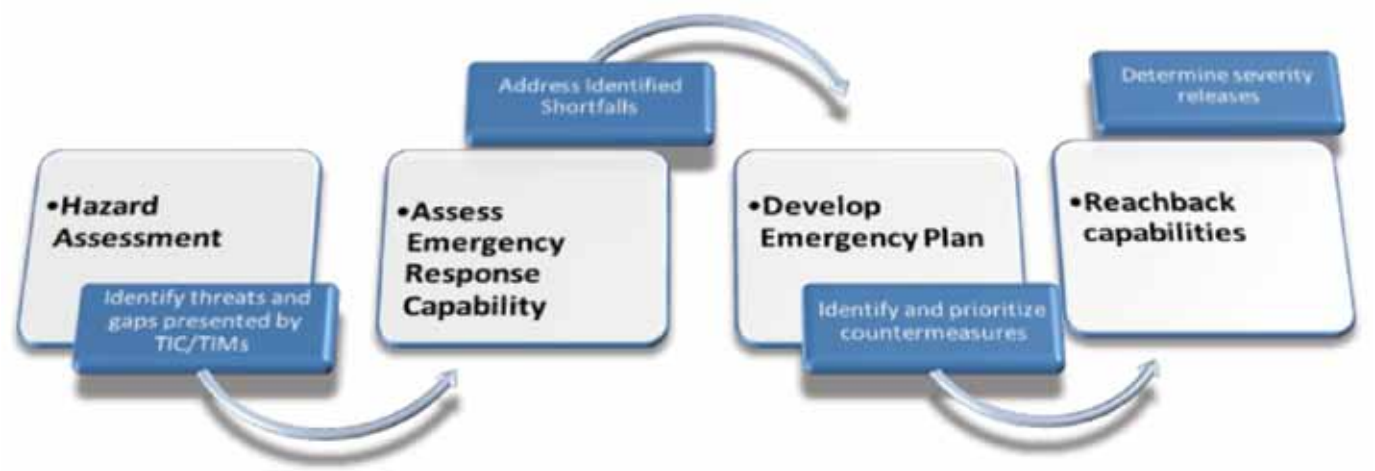
Our nation's railways connect thousands of U.S. manufacturing and chemical facilities. Consequently, freight trains move the overwhelming majority of HAZMAT transported in this country. Certain characteristics of the freight rail system make it inherently vulnerable and difficult to secure. Specifically, America's rail network is an open system, with expanses of infrastructure spread over vast regions, that traverses densely populated urban areas. In addition, railroads operate along thousands of miles of track that are generally unprotected by fences or other physical barriers. Thus freight trains and individual railcars can be especially difficult to secure in transit. Trains and railcars often travel across multiple rail lines and sometimes sit at points of connection awaiting further shipment. This can be of particular concern for railcars carrying HAZMAT because many rail yards and storage locations are located close to densely populated areas and may contain dozens of loaded HAZMAT tank cars at any given time. The difficulty and cost associated with physically securing rail yards can leave these cars easily accessible to trespassers.

Terrorists Can and Do Target Rail Systems

Although no rail incidents in the United States have been linked to terrorism, numerous suspicious incidents connected to U.S. rail systems have been reported each year. Most involved vandalism or track tampering. On 13 December 2011, for example, a train conductor in Bristol, Tennessee, reported that someone had deliberately sabotaged a train, causing 16 freight cars to detach from the train. In the ensuing investigation, knuckle pins and other metal items were noted as missing.[3] Tampering with or obstructing tracks can seriously damage or disrupt transit equipment and operations as well as injure or kill operators and passengers.

America's rail network is an open system, with expanses of infrastructure spread over vast regions, that traverses densely populated urban areas. In addition, railroads operate along thousands of miles of track that are generally unprotected by fences or other physical barriers.

In May 2011, the Department of Homeland Security



released a press release that warned of al Qaeda plots against the U.S. rail sector. The nature of the products transported, the quantities transported, and the vulnerability of rail lines make industrial transport a very attractive target for criminals or terrorists.[4]

In November 2009, 16 fuel-laden tanker cars and 300 meters of track were destroyed when suspected insurgents triggered an improvised explosive device in Assam, India. In March 2010, terrorists in the Republic of Dagestan in Russia blew up a freight train using a homemade, pressure-activated device containing approximately 2 kilograms of TNT. The explosion set fire to the locomotive, derailed it, and damaged 250 meters of track.[5]

A successful attack on a freight railcar transporting TIH through a densely populated area could meet al Qaeda's strategic goal of attacking targets that would generate mass casualties, cause economic damage, and spread fear. As of February 2010, al Qaeda was allegedly considering an attack plan that involved tampering with railroad tracks.

In October 2011, a train derailed and caught fire near a small Illinois town. The train car, which was carrying denatured alcohol, ruptured during the derailment. The subsequent explosions were deemed a danger to 800 residents, and the town was evacuated. The results of a coordinated attack involving a similar payload and targeting a more populated area could be catastrophic.[6]

Derailments Near Military Installations Demonstrate the Necessity of Planning for a Potential Rail Incident

In July 2010, a nine-car derailment resulted in a rail tank-car explosion due to operator error. Three cars erupted into fire; they contained hydrocarbons and carbon black, which are highly flammable and can cause skin irritation. This incident occurred only 10 miles from the U.S. Army Lake City Ammunition Plant.[7]

In April 2011, a car-liner failure resulted in release of 100 gallons of hydrochloric acid. Local officials issued a mandatory evacuation of 255 homes; clean-up efforts took several days. This incident occurred only 4 miles from the U.S. Air Force Academy.[8]

In July 2011, a 70-car derailment (14 cars were carrying HAZMAT) resulted in mandatory evacuation of 100 homes. This incident occurred only 18 miles from U.S. Air Force Plant 42 and 15 miles from Edwards Air Force Base.[9]

Conducting a Hazard Assessment

DoD Instruction 6055.17, "DoDI Emergency Management (IEM) Program," states that installations must conduct an annual hazard assessment to identify hazards and associated risk to personnel, property, and structures to improve protection from natural or manmade disasters or hazards.[10]

Hazard assessments serve as a foundational component for effective emergency management activities, including planning, resource management, capability development, populace education, and training and exercise. To conduct a comprehensive all-hazards assessment,

In October 2011, a train derailed and caught fire near a small Illinois town. The train car, which was carrying denatured alcohol, ruptured during the derailment. The subsequent explosions were deemed a danger to 800 residents, and the town was evacuated. The results of a coordinated attack involving a similar payload and targeting a more populated area could be catastrophic.

the probability of natural, accidental, and intentional causes that could result in a release must be assessed. Additionally, the majority of the infrastructure typically evaluated is not owned by the installation, so many traditional deterrent and preventive countermeasures are not viable options. Countermeasure recommendations should be focused on actionable planning, preparation, and mitigation such as protective actions.

Identification of HAZMAT and quantities within close proximity to an installation is a vital component of the planning process, which should also include assessing and analyzing the risk, implementing control measures, and developing recommendations to mitigate adverse impact on military operations and personnel. A

risk-based approach to planning assists decisionmakers in prioritizing resource allocation for countering these types of threats.

Having the Right Information

There has always been friction between keeping HAZMAT secure on the railroad and giving local communities the information they need during an incident. For security and proprietary reasons, railroad companies will not disclose exactly what their tank cars are carrying, specific times of transit, or locations. Generally, that means locals may not have visibility into what materials are transported through their towns. Although still a challenge today, information exchange between rail officials and locals has dramatically improved.

Numerous sources exist for acquiring information needed in the hazard assessment. Information is collected by local emergency planning committees (LEPC) and their higher state emergency response commissions (SERCs). This includes SARA Title III Tier I/II data submitted to the SERC and LEPCs. The Emergency Planning and Community Right-to-Know Act, administered by the U.S. Environmental Protection Agency (EPA), requires that detailed information about hazardous substances exceeding an established threshold in or near communities be available at the public's request. LEPCs use data collected to develop emergency plans for responding to and recovering from a HAZMAT release or spill; SERCs review and approve these plans. Information for your community can be found at the Right-To-Know Network and through EPA resources such as the Toxics Release Inventory (TRI) Database.

LEPCs also conduct commodity-flow surveys of HAZMAT transported through their jurisdictions by highway, pipeline, and railway. Risk of a chemical accident is higher when the substance is not in a secure stationary facility. The first step of a commodity-flow survey is to request information from the railroads and pipelines on their traffic amounts and materials. Out of concern for public safety against terrorist or criminal acts, these reports are released only to public safety officials. Having a member of the installation emergency management working group serve on the LEPC board allows direct access to critical information and enhances emergency planning.

Conducting a Capability Assessment and Developing a Plan

No one community or installation has sufficient law enforcement, fire, medical, rescue, and other trained personnel to cope with a major rail emergency. The severity of the disaster may be of such magnitude that additional assistance may be required from local, state, and and/or federal resources. Depending on the location of the emergency and the materials involved, there may be a need to implement other emergency response plans, and recovery operations will likely involve multiple agencies over several operational periods. To ensure that an adequate response can be accomplished, preplanning must focus on potential resource and logistics requirements. This includes assessing the installation's current capabilities and then determining the specific response, equipment, and supplies required for HAZMAT response.

When forming a rail emergency response plan, be sure to address the following issues:

- **Does the plan—**
  - Identify each separate railroad in the response area?
  - Include a capabilities assessment reflecting organic and mutual aid resources?
  - Include identified primary gathering facilities, mission-essential facilities, and areas that may be required to shelter in place?
  - Preidentify worst-case plume modeling?
  - Include accurate emergency contact information for each railroad?
  - Incorporate railroad milepost locations on response maps?

- **Ensure that the plan is continually reviewed, verified, and updated with changes.**

A comprehensive emergency plan involving a railroad should provide guidance for quick determination of the precise incident location (incorporate railroad mileposts), identification of the best access and staging areas, multijurisdictional coordination, potential for mass causalities and, if necessary, evacuation of passengers. Consideration must be given to potential HAZMAT releases that may require the installation to shelter in place. Emergency management should be prepared for the worst-case scenario. Ignoring the railroad in your emergency plans would be like ignoring a major interstate highway or airport in your jurisdiction. Understanding railroad basics can significantly enhance emergency response.

Tapping into Reachback Capabilities

Remember that the members of the railroad response team and their contractors are not far away. The Center for Toxicology and Environmental Health is one such resource and, for large incidents with a vapor release, will be on scene for long-term air monitoring and reporting. Additional resources are outlined in Table 1.

Table 1: Tapping into Reachback Capabilities

Resource	Capabilities
RAILROAD EMERGENCY CENTERS	• Can provide on-scene personnel, such a HAZMAT response personnel and railroad police, to assist with the emergency • Have detailed Geographic Information System capabilities—within minutes of a call, can make available detailed maps and information on your location, including utilities, roads and infrastructure, soil types, streams, waterways, environmentally sensitive areas, schools, and hospitals • Can also assist with plume modeling of suspected or verified HAZMAT releases
CHEMTREC	• Establishes direct communication between chemical, medical, toxicological, and HAZMAT experts and the responders at the scene of an incident • Also available to participate in local exercises through the HAZMAT exercise program
DEFENSE THREAT REDUCTION AGENCY (DTRA) REACHBACK OPERATIONS CENTER	• Generates plume modeling to accurately pre-plan and predict effects of a HAZMAT release and its impact on civilian and military populations
TRANSCAER (TRANSPORTATION COMMUNITY AWARENESS AND EMERGENCY RESPONSE	• Encourages patrnerships between citizens and industry • Helps emergency planning groups identify general types of HAZMAT moving through their community • Provides guidance for local officials to develop and evaluate the community emergency response plan • Assists with preparedness training and testing

Conclusion

The probability of rail incidents occurring naturally, accidentally, or intentionally is determined by railway safety programs, operator training, and infrastructure maintenance and security. Large trains transporting thousands of gallons of toxic material would be attractive targets for terrorist attack. As manufacturers seek cost-cutting measures, freight rail will undoubtedly become a more appealing way to transport goods; a resulting increase in rail traffic will likely increase the propensity for accidents and incidents.

Conducting a comprehensive hazard assessment will highlight areas in which your installation can better prepare for hazards and provide commanders with actionable countermeasures, which can improve continuity of operations, emergency response, and recovery from HAZMAT incidents.

To mount an adequate and efficient response, there should be continual review and upgrade of plans and procedures, additional training of personnel, and more exercise and reevaluation of capabilities. Ensuring that emergency plans identify organic and mutual-aid response capabilities, protocols, and procedures will minimize the impact on mission personnel and the surrounding community and could ultimately save lives and property.

1 MTA-83411-2011-03-01.

2 Cease, John. "Why Emergency Response Plans Should Include the Railroad." Emergency Management, 22 June 2011. Available at http://www.emergencymgmt.com/disaster/Why-Emergency-Response-Plans-Include-Railroad.html

3 Supra, 1.

4 U.S. Department of Homeland Security, "Al-Qa'ida Interest in 2010 to Attack U.S. Rail Sector," press release, 5 May 2011.

5 MTA-83411-Freight Rail Modal Threat Assessment.

6 "Town evacuated by train derailment, explosion." WLS-TV, 7 October 2011. Available at http://abclocal.go.com/wls/story?section=news/local/illinois&id=8382693

7 National Infrastructure Coordinating Center.

8 Ibid.

9 Ibid.

10 DoD Instruction 6055.17. "DoD Installation Emergency Management (IEM) Program." Available at http://www.dtic.mil/whs/directives/corres/pdf/605517p.pdf

ANTITERRORISM DOCTRINE FM 3-37.2

U.S. Navy photo by Mass Communication Specialist 3rd Class Kristopher Regan/Released

A Guide for Preventing Terrorist Attack

This article was written by staff from the Antiterrorism Branch, Office of the Provost Marshal General; Law Enforcement Branch, Office of the Provost Marshal General; and Criminal Investigation Division

In February 2011, the Army unveiled its first-ever AT doctrine, FM 3-37.2, "Antiterrorism," to instruct Soldiers on the baseline fundamentals of facing a terrorist attack.

> *Doctrine* … is a guide to action, not hard and fast rules. Its objective is to foster initiative and creative thinking. It … provides a menu of practical options based on experience from which self-aware and adaptive Army leaders can create their own solutions quickly and effectively.
> —FM 1, U.S. Army, 14 June 2005

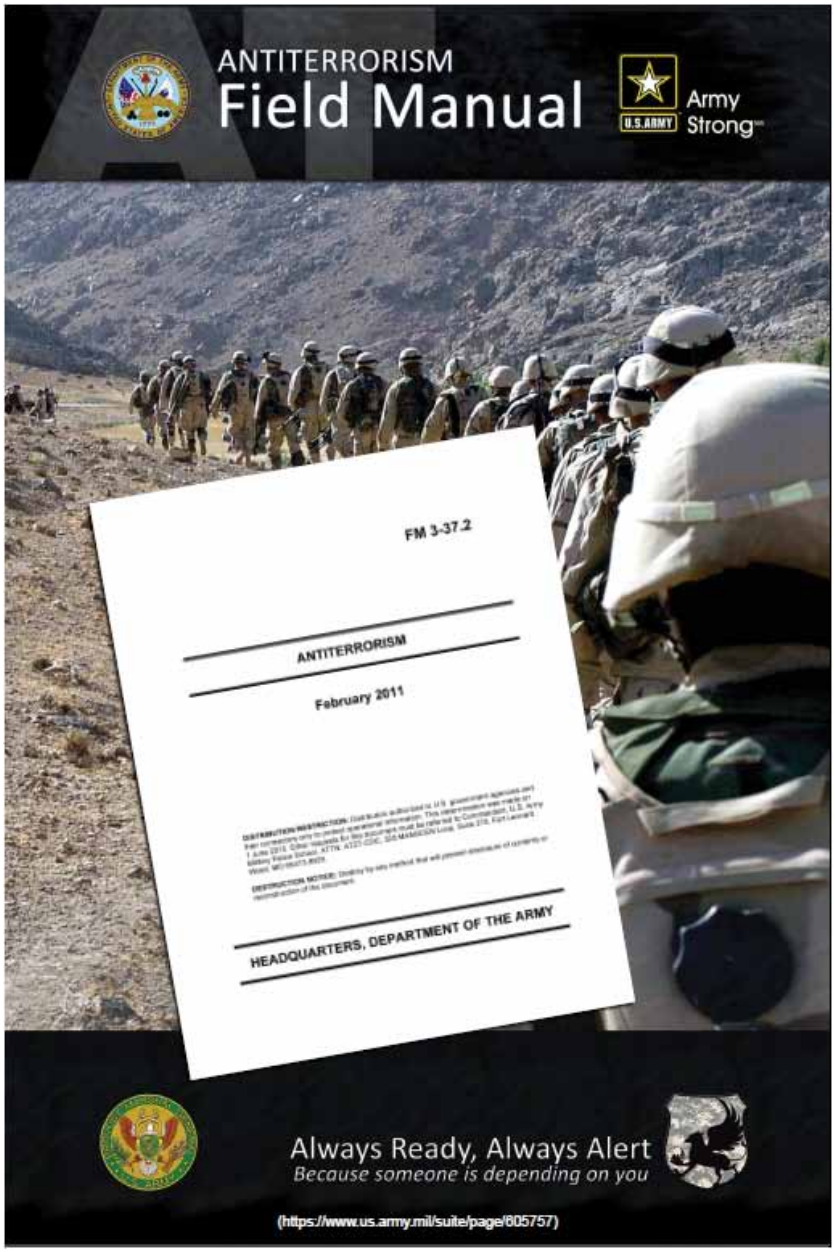
What is AT? How does it apply to my situation? What actions will prevent a terrorist attack? If I do not have enough protection assets, can I assume the associated risk? Those questions do not have precise answers; nevertheless, they are worth contemplating. Confederate cavalry commander Colonel John S. Mosby once opined that "war is not an exact science, and it is necessary to take some chances."[1] This is just as true today for preventing a terrorist attack as it was for defending against Union cavalry.

Colonel Mosby highlighted the basic challenge for all Soldiers in virtually every situation. How does a Soldier know how to act, what to do, and when to do it? Army policy provides the baseline fundamentals of what must be done. Army Regulation 525-13, "Antiterrorism," provides that baseline but does not account for the numerous possibilities driven by the security environment, the available resources, and any number of other variables. The Army guides but does not dictate

Terrorism is an enduring, persistent, worldwide threat to our nation and our Army, both at home and abroad. As we pursue terrorists around the world, we must also prevent a successful attack against the Army community. Doctrine supplies the foundation on which to build programs with that aim.

those actions through doctrine. Until recently, there was no "guide" for AT to help leaders and Soldiers answer the questions posed above. In February 2011, the Army unveiled its first-ever AT doctrine, FM 3-37.2, "Antiterrorism." Now that we are more than a year into implementing the guidance, we should reflect on its purpose to ensure understanding and to gauge how well units are doing in integrating AT doctrine into all Army operations.

Terrorism is an enduring, persistent, worldwide threat to our nation and our Army, both at home and abroad. As we pursue terrorists around the world, we must also prevent a successful attack against the Army community. Doctrine supplies the foundation on which to build programs with that aim. Within a framework bound by policy and broad principles, doctrine encourages creative solutions and resourcefulness. For the first time, Soldiers have a blueprint to help build AT plans and programs. Although it does not provide definitive answers, doctrine suggests solutions rooted in history and experience. As Theodore Roosevelt observed, "we must strike out for ourselves, we must work according to our own ideas, and we must free ourselves from the shackles of conventionality, before we can do anything."[2]



Army forces must seek to understand the threat; to detect terrorist activities; and to prevent, warn, and to defend against the full range of terrorist tactics. AT is the defensive fight against terrorists. In this fight, Army units must constantly seek improvement of their defensive postures. The remedy lies within each organization related to its mission, and doctrine can help guide the way. It offers a compass that gives direction. When coupled with the understanding known only by those facing a particular situation, doctrine represents a critical element in the formulation of an effective plan for success.

AT efforts have undergone significant changes and improvements over the past two decades. To meet a growing and evolving terrorist threat, the Army combined the most important elements of AT policy with the doctrinal wisdom and practical application of operational forces, installations, and stand-alone facilities. By leveraging extensive AT expertise from across the force, sound doctrinal principles, processes, and tools have emerged. AT FM 3-37.2 establishes AT principles, integrates AT within the combating terrorism framework and protection warfighting function, and builds on the Army's effective operations and intelligence processes.

As a militia commander in 1783, American icon Daniel Boone instructed his subordinate commanders, "If sine [sign] be found the commander must act as he thinks most prudent as you will be the best judge when on the spot."[3] Boone expressed the notion that threat warnings must be addressed according to the situation, not by prescribed rules and regulations. No two situations are ever exactly the same. Completely random solutions to unique challenges will often lead to chaotic and ineffective solutions. When guided by bedrock principles, Soldiers stand a better chance of forming effective plans.

FM 3-37.2 establishes Army AT principles to guide the key elements of AT planning, program development, and execution. The five AT principles—Assess, Detect, Defend, Warn, and Recover—contained in Chapter 3 ("Foundations of Antiterrorism") represent the characteristics of successful AT planning and operations and support the broader functional concept of protection. The AT principles guide the operational forces on how to protect units and operations from terrorist attacks and threats. Key protection measures include persistent

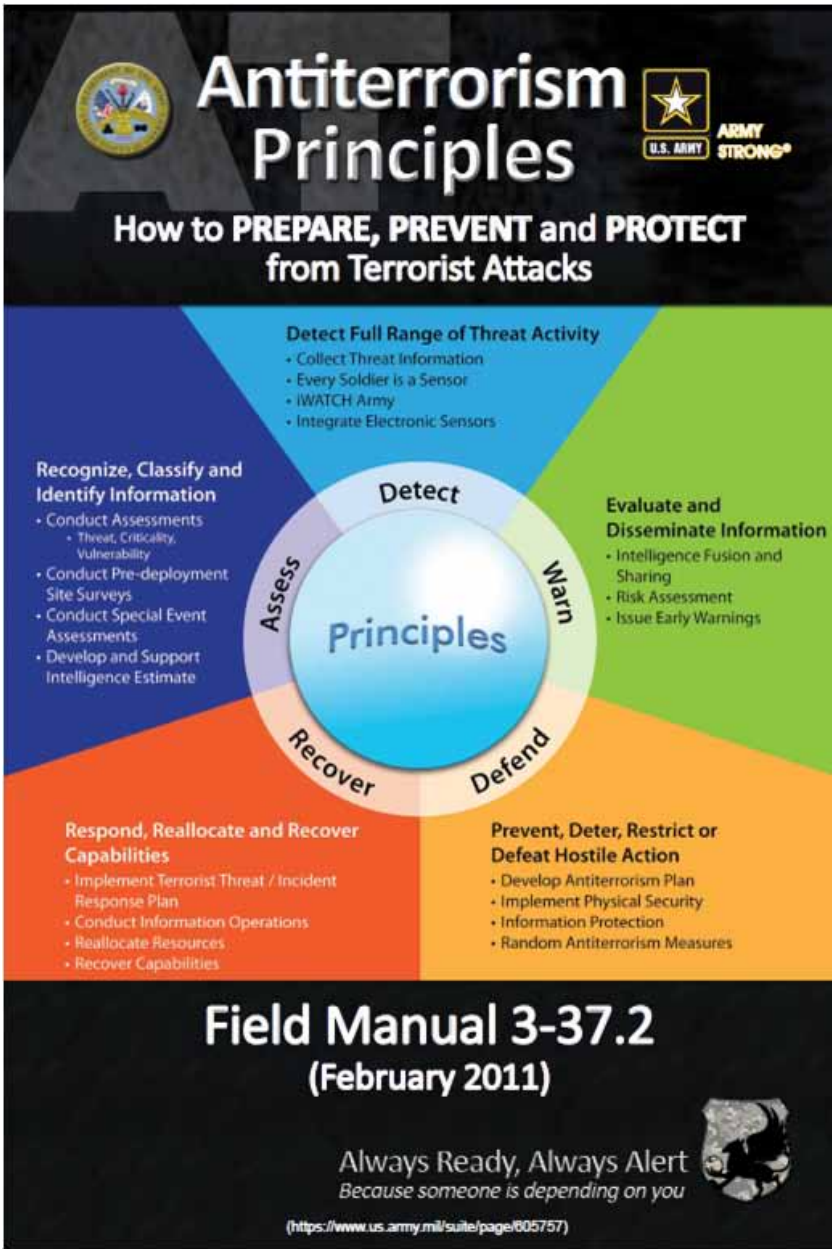
detection, shared understanding, and dissemination of threat information. The AT principles guide unit leaders toward the best approach to protect personnel, information, and critical assets by applying active and passive measures. Protection measures include integrating elements of other security programs, such as physical security, military and criminal intelligence, law enforcement, information assurance, operations security, and emergency management.

The AT doctrinal manual helps commanders and units integrate AT concepts and principles across the full spectrum of operations, defend against the terrorist threat, develop AT awareness programs, and provide AT officers with an approved doctrinal reference to better guide and support their units.

To reinforce the Army's newest AT doctrine, Headquarters, U.S. Department of the Army, AT Branch, established a supporting AT strategic communication (SC) theme and products. The purpose of the theme is to encourage Army forces to embrace the doctrine, focusing initially on AT principles, planning, exercises, assessments, and supporting AT SC plans. The AT doctrinal theme received Armywide focus during the fourth quarter of fiscal year 2011 as well as throughout the second annual AT Awareness Month in August 2011. Products and tools to support educating the field on the AT doctrinal manual include a series of doctrine posters to advertise the release of FM 3-37.2 and AT principles, planning, exercises, and assessments as well as a how-to primer for developing AT strategic communication plans. These products and much more AT information are available at Army Knowledge Online (https://www.us.army.mil/suite/page/605757).

Integrating AT doctrinal principles with constant AT awareness will ensure the safety and security of the Army community while facilitating mission success. AT Awareness Month and the implementation of an AT SC theme provided the opportunity for Army forces to dedicate efforts to understanding a critical element of doctrine that affects full-spectrum operations. Units and leaders should pause to consider how well they have embraced the new doctrine and what more can be done.

As the Army institutionalizes FM 3-37.2, we must continue to capture lessons learned and best practices for continuous improvement. Legendary basketball coach John Wooden captured his concept of success in his memoirs: "There is no stronger steel than the well-founded self-belief; the knowledge that your preparation is complete."[4] By using AT doctrine, analyzing the peculiarities of a situation, and applying resourceful solutions, the Army can build a "steel" foundation and complete preparations to prevent successful terrorist attacks.



1 Mosby John. Gray Ghost, Memoirs of Colonel John Mosby. (Charles Wells ed., Little, Brown 1917, p. 125).

2 Roosevelt, Theodore. Theodore Roosevelt: Letters and Speeches. (Louis Auchincloss ed., Library of America 2004, p. 59).

3 Faraghar, John Mack. Daniel Boone. (Holt Paperbacks 1993, p. 250).

4 Wooden, John, & Steve Jamison, Wooden on Leadership: How to Create a Winning Organization. (McGraw-Hill 2005, p. 51).

FALLACY OF SECURITY

(U.S. Air Force Photo/Master Sgt Scott T. Sturkol/Released)

A robust security posture does not necessarily deter terrorist attackers

By Ben Nerud, Defense Threat Reduction Agency, Deputy Chief, Base Survivability Assessments Branch, and Jeffrey R. Benton, HQ Defense Logistics Agency Antiterrorism Team

Conventional—and outdated—widsom regarding target vulnerability must be replaced by an attack-prevention system.

Conventional wisdom is a term used to describe ideas or explanations generally accepted as true by the public or by experts in a field.[1] The security industry, and AT in particular, seems to thrive on three "accepted truths":

(1) Terrorists attack soft targets.

(2) A robust security posture is a deterrent.

(3) When faced with a choice between two targets, terrorists will always select the target with the least amount of security (the old "make him attack the other guy" theory).

Here is the problem: Conventional wisdom is not current wisdom. None of these accepted truths matches reality. Terrorists select targets based on a myriad of factors with the primary considerations of compliance with their doctrine, strategy and goals, the ability of the attack to influence a specific audience, demonstrations of their strength, and revenge—all to coerce a society or to exact concessions to create their own special brand of utopia.

Consider the current trend of high-profile attacks. The target list has included embassies, military bases, government buildings, police stations, and, of course, airlines. None of these could be considered soft targets, yet all were chosen and were successfully attacked. Why do we say successfully? The terrorists determine the criteria for selecting a target; therefore, they determine the conditions for success. The victim merely gets to say, "Well, they didn't kill that many people," or "It could have been much worse." A robust security posture did not deter the terrorists. A statement from the al Qaeda organization in the southern Arabian Peninsula revealing details of the 17 September 2008 attack on the U.S. Embassy in Sana'a, Yemen reads: "Let everyone know that this attack did not take place in a market where Muslims frequent or one of their gathering spots or homes. This took place in the pit of deviousness and

treachery, a fortified base of the Global Crusaders."[2] This statement shows that the robust security posture actually made the target more attractive. The sixth issue of the jihadist magazine *Sada al Malahim* published an analysis of the same attack, stating that the embassy was "the strongest fortified place in Yemen"[3]—so much for choosing the target with the least amount of security.

Within our conventional wisdom lies the fallacy of security. To correct these false truths, we must change from conventional wisdom to current wisdom. In the 4th century B.C., Sun Tzu wrote in *The Art of War,* "So to win a hundred victories in a hundred battles is not the highest excellence; the highest excellence is to subdue the enemy's army without fighting at all."[4] How do we, from an AT perspective, subdue the enemy without a fight? We deny terrorists the ability to attack. Denying the ability to attack requires selection and implementation of a series of countermeasures that not only protect our assets but also disrupt the entire operational cycle of the terrorists. We will call this new spin on defense-in-depth an attack-prevention system. First, we will examine our current protection schemes.

How do we, from an AT perspective, subdue the enemy without a fight? We deny terrorists the ability to attack. Denying the ability to attack requires selection and implementation of a series of countermeasures that not only protect our assets but also disrupt the entire operational cycle of the terrorists.

Current Protection Schemes

Our current protection systems normally begin at our perimeter and shift inward toward our critical assets. They consist of a series of countermeasures designed to detect, delay, deny, and defeat an adversarial attack; failing this, we include response countermeasures and contingency plans to respond and recover from an attack. This is classic defense-in-depth, or integrated security, encompassing both physical and procedural measures to thwart an attack. This security system relies on the expectations associated with the three "truths" of conventional wisdom: If enough security—guards, guns, and gates—is in place, it is adequate to deter a terrorist.

Because of the conventional wisdom perspective, measures that actually influence the terrorist's operational cycle, such as random AT measures (RAMs), surveillance detection and countersurveillance, and intelligence gathering, are given only enough thought and effort to satisfy the requirement of passing a vulnerability assessment. On numerous occasions, for example, the authors were informed that the only function of an installation RAM program was to test and validate measures from a higher FP condition, not to actually deter terrorist attacks.

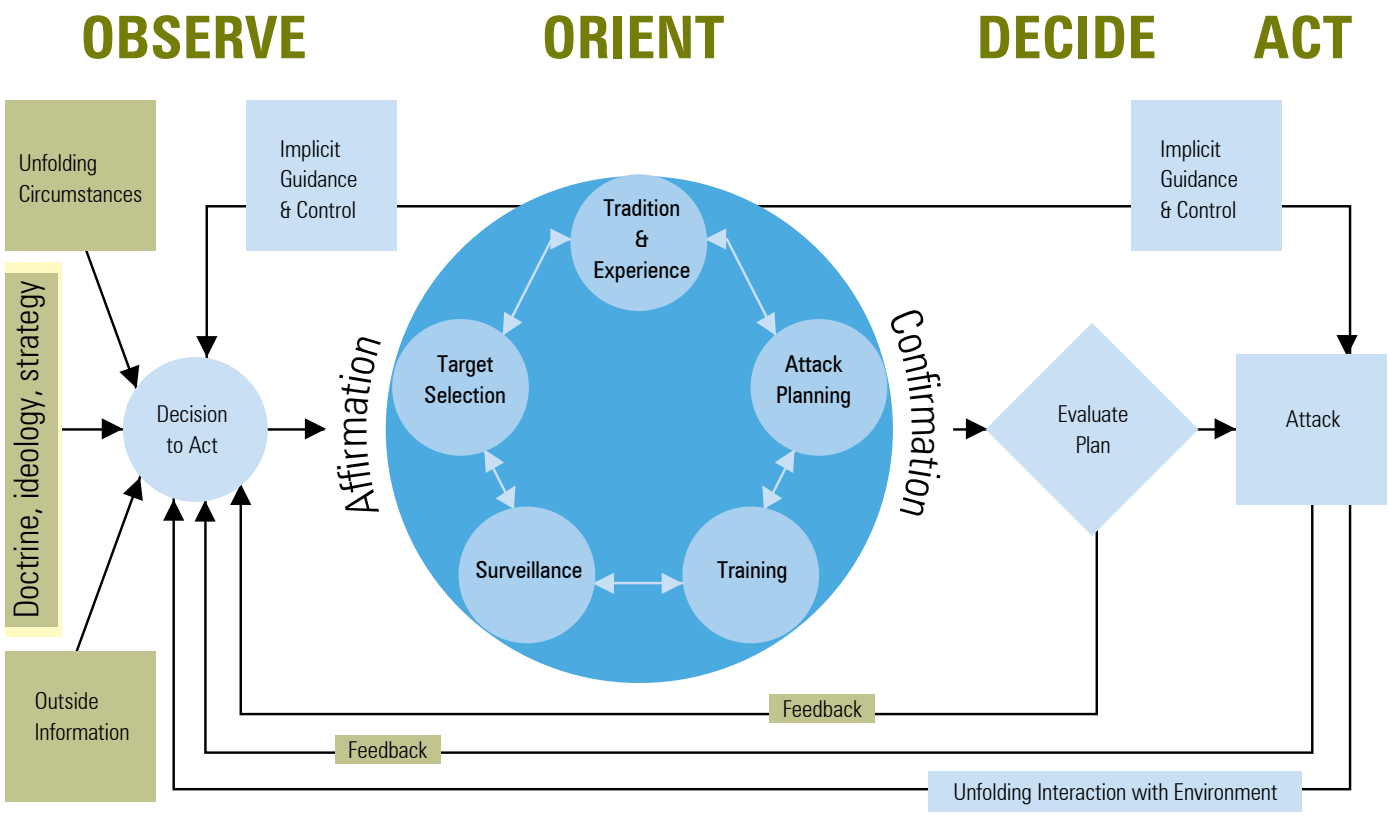
Traditional approaches to protection, based on the belief in the truths of conventional wisdom, reflect a cognitive bias that hinders the development of countermeasure strategies. Rather than base protective design on current wisdom, we frame our situational awareness in a way that allows us to adapt it to traditional security approaches. This does not mean that we deliberately ignore current wisdom, and it does not mean we do not recognize the necessity of adapting our protective strategies; we just are not doing anything about it. The result is protective programs that continue to be reactive rather than proactive. How can we change this? We can modify our strategy from attack protection and response to attack prevention.

The Attack Prevention System Concept

An attack prevention system incorporates layered countermeasures designed to affect critical nodes within the terrorist's attack cycle. These countermeasures affect these nodes by four basic means. The first countermeasure layer affects the behavior of the adversary. Essentially, these countermeasures influence behavior by limiting the terrorist's ability to gather information or the freedom of movement necessary to gather the data. This type of effect is the most proactive because it directly affects the ability of adversaries to orient themselves. The second countermeasure layer affects the operational capability of the terrorist. These measures restrict the ability of the terrorist to perform the required tasks necessary to develop an attack course of action. The third countermeasure layer limits the courses of action available to the terrorist. These countermeasures consist of physical and procedural measures specifically designed to disrupt terrorist planning efforts. The final countermeasure layer consists of the traditional security measures designed to defend against an attack. These measures are the guards, guns, and gates of the physical security system. This countermeasure layer provides some deterrence; however, our adversaries use surveillance and planning to defeat these measures. Their real benefit lies in their ability to defeat an attack.

Developing an attack-prevention system begins with an understanding and analysis of the adversary's attack cycle. Although case studies of attacks should provide these data, all too often they merely focus on how the security system failed. These studies may address some of the adversary's activities that took place in preparation for the attack but usually are confined to the attack, corresponding damage, and a litany of lessons learned. These lessons normally take the form of broad statements that identify a problem but do little to identify specific corrective action. Of these broad statements, one of the more frequently touted concepts is, "We need to get inside their loop." The key to getting inside the loop is effective analysis based on current wisdom and the application of measures to disrupt the adversary's Observe, Orient, Decide, Act (OODA) Loop.

Figure 1: Terrorist OODA Loop[6]



Observe–Orient–Decide–Act

Air Force Col John Boyd (deceased) developed the OODA Loop to describe the decision cycle process by which an entity reacts to an event. He broke this process down to a simple four-step, iterative cycle: Observe–Orient–Decide–Act (Figure 1). The theory behind the process is that prior to taking action, a decisionmaker must observe a condition, situation, or opportunity that requires action. To act effectively, the decisionmaker orients himself or herself to the condition. Orientation is based on the decisionmaker's capability to analyze and synthesize his or her training, previous experience, and cultural traditions with the new information obtained. Once oriented, the decisionmaker evaluates the options available, chooses one, and then acts. The process repeats itself until resolution is achieved.

As part of this process, Boyd identified the means of defeating an adversary: to have a faster OODA Loop cycle than the adversary, forcing the adversary to react to you while you maintain the initiative. In *Discourse on Winning and Losing*, Boyd described this concept: "Without the ability to get inside other OODA Loops (or other environments), we will find it impossible to comprehend, shape, adapt to, and in turn be shaped by unfolding, evolving reality that is uncertain, ever-changing, unpredictable."[5]

Boyd's OODA Loop provides a means of evaluating the decisionmaking process, but it is not sufficiently detailed enough to use as an analytic model by itself. The purpose of intelligence analysis methods is to create a model of the target to obtain information to defeat the target. This analysis requires two components: (1) the identification of critical nodes within the adversary's OODA Loop and (2) the application of mechanisms to defeat or disrupt those nodes.

The OODA Loop can incorporate many models to aid in the identification of its critical nodes. One method identifies critical capabilities and the critical requirements of those capabilities to determine which nodes are vulnerable to defeat mechanisms. Dr. Joseph Strange of the Marine Corps War College and Colonel Richard Iron, U.K. Army, developed this framework in their paper, *Understanding Centers of Gravity and Critical Vulnerabilities*.[7]

Dr. Strange expanded on the Clausewitzian concept of centers of gravity, providing a means of dissecting an adversary's operational system or significant portions of it. This process encompasses a tiered approach, establishing the adversary's center of gravity—the primary source of moral and physical strength, power, and resistance. Within these centers of gravity are the crucial enablers, critical capabilities. For critical capabilities to function, essential conditions, resources, and means must be present. These conditions, resources, and means constitute critical requirements.

Within an OODA Loop, critical capabilities are the ways by which an adversary observes, orients, decides, and acts. Critical requirements are the means and

resources necessary for the adversary to accomplish individual critical capabilities. Understanding all aspects of the adversary—capabilities, tactics, and decisionmaking processes—is essential to getting inside the OODA Loop. Identifying critical capabilities and requirements establishes this nexus (Figure 2).

After breaking down an adversary's system, an analysis of each node determines its vulnerability to defeat mechanisms. Nodes susceptible to influence constitute critical vulnerabilities. The application of defeat mechanisms at these points degrades or denies the critical requirement, thereby disrupting the adversary's OODA Loop.

Perhaps the key capability to disrupt is the adversary's Orient phase. Orientation is the ability to adjust or align oneself or one's ideas according to new surroundings or circumstances. Defeating the Orient phase requires the application of mechanisms to create an environment in which adversaries either cannot orient themselves or orient themselves incorrectly, causing them to make inappropriate decisions. Poor decisions may cause an adversary to fail to achieve an objective or to act in a manner that can be defeated easily.

Three methods are used to influence a critical requirement. BG Huba Wass de Czege (Ret.) identified these methods, referring to them as defeat mechanisms. They consist of attrition, disintegration, and dislocation.[8] Attrition reduces an adversary's manpower or resources using destructive force. Disintegration reduces the adversary's manpower or resources by influencing the support systems necessary for an adversary to act. Dislocation changes the environment in which the adversary must operate, affecting the ability to maintain the initiative and freedom of movement.

Identifying and implementing defeat mechanisms or strategies requires careful analysis to apply the correct measures against nodes that are susceptible to influence by those measures. Pitting the wrong defeat mechanism against the wrong node is useless at best or, worse, provides the adversary with greater moral or physical

Figure 2: Author's Illustration of the al Qaeda Center of Gravity (CG), Critical Capability (CC), Critical Requirement (CR) Analysis

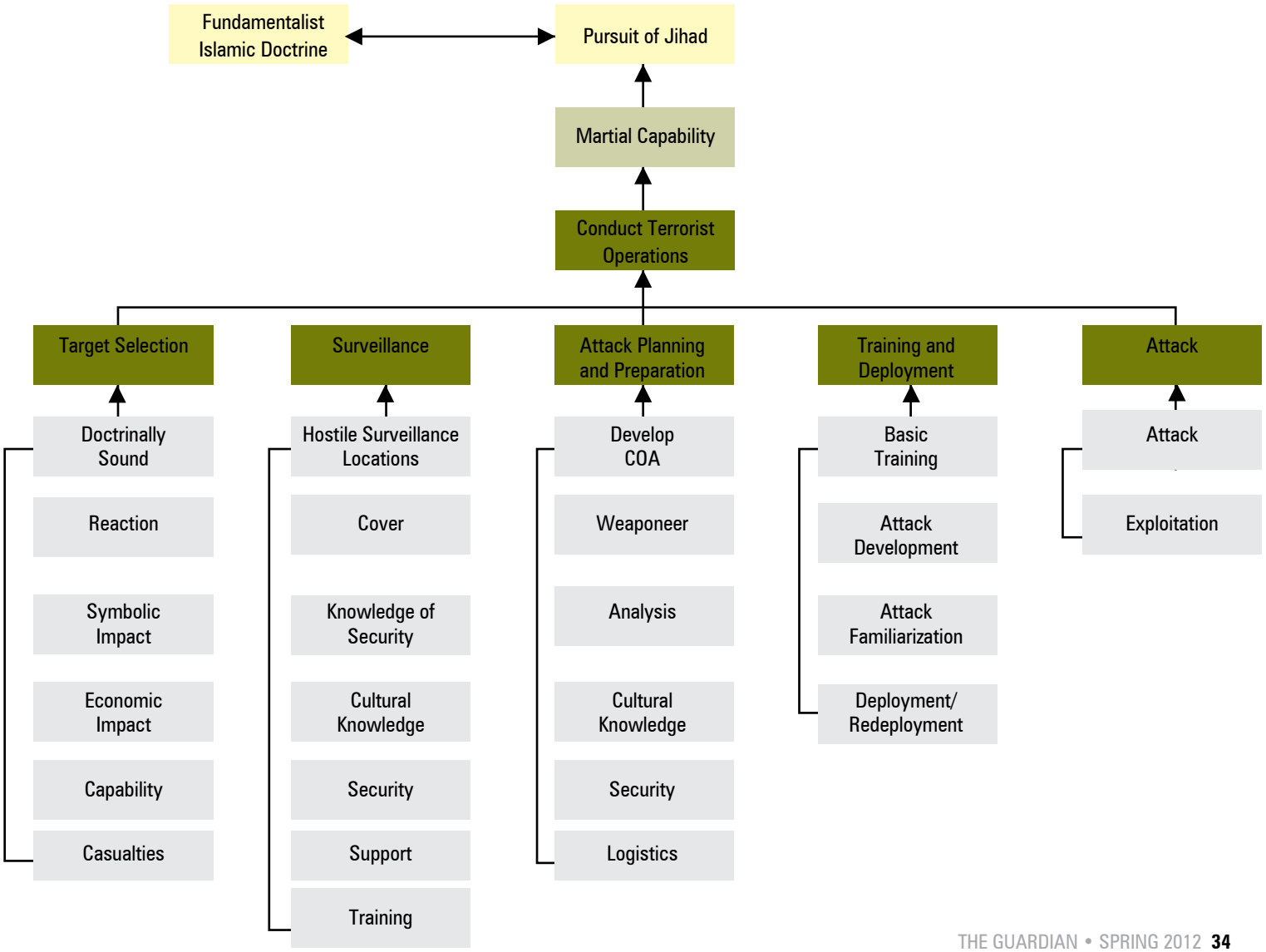


Figure 3: Attrition Countermeasures

Countermeasure
Limit available information through robust OPSEC Program
Reduce hostile surveillance locations by elimination or obscuration

Adversary Response
Forces terrorists to use aggressive information-gathering techniques or to use less than optimal surveillance locations; requires terrorists to make unverifiable assumptions

Impact on Adversary
Increased risk of detection in early stage of attack cycle; questionable data gathered; affects ability to orient

Adversary Counteraction
Increased time spent on surveillance; cover becomes primary consideration; reliance on generic open source information

strength.

Defeat mechanisms should be capable of disabling the nodes required by the adversary. To do this, defeat mechanisms must be oriented as part of a system. The more complex the adversary, the greater the need to develop coordinated defeat systems that use multiple defeat mechanisms targeted against multiple critical vulnerabilities. Defeat mechanisms can be oriented to engage these critical vulnerabilities either sequentially or simultaneously. The entire system has one primary goal: to disrupt or deny the critical nodes necessary for the adversary to accomplish its objectives. Figures 3–6 show the cumulative effects of this type of system.

The author's illustration of four essential components have been identified as necessary to defeat an adversary. First, establish the adversary's methodology for making decisions (the OODA Loop). Second, identify the aspects of the adversary's operations that are susceptible to influence (critical capabilities and critical requirements). Third, determine what types of measures can be applied to those critical nodes to disrupt or deny them (defeat mechanisms). The final component is the evaluation of the effect of the application of specific defeat mechanisms on the overall adversarial planning and decisionmaking process (the OODA Loop).

This methodology aids planners by identifying aspects of the adversary's operations that are susceptible to defeat and aids in the selection of appropriate defeat mechanisms. To complete this process, it is necessary to identify when to implement certain defeat mechanisms to obtain the greatest effect. Using the OODA Loop, the effect of each defeat mechanism on each critical node determines the overall effect on the adversary's decisionmaking process. By determining the effect, it is possible to comprehend, shape, and adapt the environment to the planner's benefit. In other words, this methodology gets inside the adversary's OODA Loop.

Conclusion

This article expands on the concepts first introduced in "Antiterrorism and the Vacation Mindset," published in *The Guardian* in 2008 (Issue 3). The central theme

Figure 4: Dislocation Countermeasures

Countermeasure
Eliminate or limit available cover for status or action
Increase surveillance detection, exploitation, and neutralization capabilities

Adversary Response
Increased emphasis on operational security, limiting freedom of movement; perimeter and interior surveillance may not be possible; increased reliance on generic information and elicitation

Impact on Adversary
Required information becomes unavailable in early stage of attack cycle; questionable data gathering; affects ability to orient

Adversary Counteraction
Planning becomes more general, requiring aggressive plans to defeat suspected countermeasures

Figure 5: Disintegration Countermeasures

Countermeasure
Change overall physical and procedural security posture for extended periods

Adversary Response
Planning considerations changed frequently based on security changes; increased surveillance and multiple contingency plans required; success rate may drop below 75%

Impact on Adversary
Less robust planning; spur-of-the-moment operations focusing on targets of opportunity; attack familiarization and other training deficient due to lack of adequate planning

Adversary Counteraction
Increase operational tempo in order to take advantage of perceived vulnerabilities or targets of opportunity; reliance on traditional or stand-off attacks

Figure 6: Traditional Countermeasures

Countermeasure
Robust security posture designed to detect, delay, and defend against attacks

Adversary Response
Lengthen time allocated to planning and training; aggressive attack methods or use of stand-off attacks

Impact on Adversary
Requires increased surveillance and information collection; comprehensive planning; extensive training

Adversary Counteraction
Re-engage entire spectrum of attack

of both articles reflects the difference between our perceived protection and actual protection. Realistically, the probability of a specific asset becoming the target of a terrorist attack is extremely low; however, the potential exists and the consequences are catastrophic. Creating attack-prevention systems, rather than just a robust protection posture, lowers the possibility of being selected as a terrorist target even further because the countermeasures implemented affect not only the requirements they are designed to disrupt or deny but also the critical requirements within the target selection process. The doctrine, tools, tactics, and resources necessary to create attack prevention systems exist and are available to every security program; however, the application is obscured by conventional wisdom. Reevaluating generally accepted truths and focusing on current wisdom allow our protection strategies to surpass the capability and intent of our adversaries.

1 Merriam-Webster Online Dictionary. "Conventional Wisdom." http://www.merriam-webster.com/dictionary/conventional%20wisdom

2 Makram, Faysal. "Al-Qa'ida in Yemen: Seven Not 6 Suicide Bombers Attacked US Embassy." Al-Hayah Online, 10 November 2010.

3 al-San'a'I, Abu Hurayrah. "The Indications of the Embassy Operation." Islamic Al Fallujah Forums. Available at www.al-faloja.info

4 Tzu, Sun. The Art of War. (Denma Translation Group ed.)

5 Col John Boyd's theories on warfare consist of a presentation of several hundred slides entitled, "Discourse on Winning and Losing," and a short essay entitled, "Destruction and Creation" (1976).

6 Author's adaptation of Boyd's OODA Loop construct depicting terrorist operational cycle. Original OODA Loop construct can be found at: http://pogoarchives.org/m/dni/john_boyd_compendium/essence_of_winning_losing.pdf

7 Strange, Joe, & Richard Iron. "Understanding Centers of Gravity and Critical Vulnerabilities." Available at http://www.au.af.mil/au/awc/awcgate/usmc/cog2.pdf

8 "DEFEATING A CAUSE: ANATOMY OF DEFEAT FOR CONFLICTS INVOLVING NON-NATION-STATES, A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree MASTER OF MILITARY ART AND SCIENCE General Studies by STEVEN M. SALLOT, MAJ, USA," http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA452043

Additional Resources

LEVEL I AT TRAINING
https://atlevel1.dtic.mil/at

CJCS Level IV Antiterrorism Executive Seminar (Nomination Required)
https://www.intelink.gov/sites/atlevel4/default.aspx/

RAND CORP
http://www.rand.org/research_areas/terrorism/

OPEN SOURCE INTELLIGENCE/PUBLICATIONS
http://www.fas.org/irp/offdocs/index.html

DoD DIRECTIVES/INSTRUCTIONS
http://www.dtic.mil/whs/directives

GOVERNMENT ACCOUNTABILITY OFFICE (GAO)
http://www.gao.gov

ASD (SO/LIC&IC)
http://policy.defense.gov/solic/index.aspx

ASD (HD&ASA)
http://policy.defense.gov/hdasa/index.aspx

National Counterterrorism Center
http://www.nctc.gov/

US ARMY – AT PROGRAM
https://www.army.mil/suite/page/605757

ARMY KNOWLEDGE ONLINE (AKO)
https://www.us.army.mil

NAVY AT/FP PROGRAM
https://portal.navfac.navy.mil/portal/page/portal/navfac/navfac_ww_pp/navfac_nfesc_pp/atfp

COMBATING TERRORISM CENTER AT WEST POINT
http://www.ctc.usma.edu/

USAF AT/FP PROGRAM
http://www.e-publishing.af.mil/shared/media/epubs/AFI10-245.pdf

Combating Terrorism Technical Support Office (CTTSO)
http://www.cttso.gov/

Technical Support Working Group (TSWG)
http://www.tswg.gov/

Biometrics Identity Management Agency (BIMA)
http://www.biometrics.dod.mil/

Joint IED Defeat Organization (JIEDDO)
https://www.jieddo.dod.mil/index.aspx

FBI MOST WANTED TERRORISTS
http://www.fbi.gov/wanted/wanted_terrorists

GLOBAL TERRORISM DATABASE
http://www.start.umd.edu/gtd/

DHS COUNTERTERRORISM
http://www.dhs.gov/files/counterterrorism.shtm

DHS NATIONAL TERRORISM ADVISORY SYSTEM (NTAS)
http://www.dhs.gov/files/programs/ntas.shtm

JOINT TERRORISM TASK FORCE
http://www.justice.gov/jttf/

J-34, Deputy Directorate for Antiterrorism/Homeland Defense

DD AT/HD	MG Jeff W. Mathis	703-695-8452
ADD	Col Gregory Thomas	703-693-7555
Chief of Staff	Mr. Andrew Huddleston	703-697-9499
DDAT/HD-EA	LtCol David E. Morgan	703-697-9444
Admin Asst.	YNC Catrina Dural	703-695-6516
Admin Asst.	SFC Michelle Burckhalter	703-693-7503
Admin NCOIC	SFC Eligia Smith	703-693-7501

Antiterrorism/Force Protection

ADD AT/FP	CAPT David Bossert	703-697-1982
	COL Michael Brobeck	703-641-1273

AT/FP Programs Branch	Lt Col Eric Knapp	703-693-7535
	Lt Col Nathan Schalles	703-614-0083
	LTC Brock Jones	703-693-7562
	LCDR Alexander Korn	703-693-7521
DCIP, Resources and Assessments Branch	LTC Michelle McCassey	703-614-4094
	Mr. Brian Bell	703-693-7551
	Mr. David Johnson	703-614-1280
	SGM Rosemary Helton	703-693-2111
AT/FP Policy and Training Branch	Mr. Michael Osterhoudt	703-693-7526
	LCDR Matthew Thomas	703-614-1276
	LCDR Paul Will	703-693-1454
	SMSgt Walter Weatherford	703-693-7542

JDOMS Division	COL William Steinkirchner	703-695-8453
	Mr. Joseph Austin	703-692-6350
	Mr. Michael Avila	703-697-0879
	LtCol Robert Jackson	703-693-0663
	Lt Col Robert Pata	703-697-9439
	LTC Vanessa Gattis	703-693-5446
	CDR Robert Toth	703-693-0675
	Mr. Glen Stagnitta	703-693-5736
	Mrs. Jamie Zawadski	703-693-0679
	Mr. John Wood	703-692-6349
	Ms. Deidre Matthews	703-693-0678
	Mr. Glen Stagnitta	703-693-5736
	LTC Erik Rude	703-693-8813
LNO to FEMA	Lt Col William Valentine	202-646-3489
CBRNE Division	LTC Michael Hedges	703-697-8215
	Mr. Carl Simchick	703-697-9459
	Mr. Harvey Hubbard	703-697-9476
	Mr. Stephen C. Malone	703-692-4546
	MAJ Bryan Carr	703-614-7969
	Dr. Allison Hinds	703-697-0914
	LTC Jeffrey Kyburz	703-697-8259
	CDR James Mason	703-693-7513
Homeland Defense/ Theater Support	CAPT Mark Frankford	703-697-8170
	CDR Andrea Palmero	703-697-8170
	LCDR Stephen Minihane	703-692-4951
	LCDR Joseph Droll	703-693-4233
	MAJ Benny Smith	703-693-4231
	MAJ Kris Kerpa	703-697-9430
	Maj Jeannette Haynie	703-692-4959
	Col John Franklin	703-697-9441
	LtCol Russel Burton	703-697-9441
	LtCol Maki Livesay	703-693-7444
	Mr. Mark Ashley	703-697-9415

DD AT/HD
Joint Staff, J-3 Operations Directorate
Pentagon
Room MB917
Washington, DC 20318-3000

Note: If your copy of the Guardian has been damaged in shipping or is unreadable, please contact us at guardian@js.pentagon.mil. We will send out an electronic pdf to replace it.