
THREAT INFORMATION
SYNCHRONIZATION
PROVOST MARSHAL GENERAL
U.S. ARMY
DEPARTMENT OF THE ARMY
UNITED STATES OF AMERICA
1775
Always Ready, Always Alert
Because someone is depending on you
U.S.ARMY
Army
Strong℠

Threat Information Synchronization

PURPOSE

This paper offers a possible methodology for the general flow of threat information and the activities involved at various levels within the Army antiterrorism (AT) community.

> "Suspicious Activity: Observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity."
>
> Information Sharing Environment Functional Standard: Suspicious Activity Reporting, Version 1 (and DoD Instruction 2000.26, Suspicious Activity Reporting, 1 November 2011)

TERRORIST PLANNING CYCLE

Although there is no universal model to reflect the terrorist planning process, **Figure 1** depicts a general cycle that terrorists modify based on specific objectives, resources, and time available. Although terrorist activities may appear as random acts, they are typically decisive and directed activities carried out by sophisticated groups who generally follow a deliberate planning cycle.

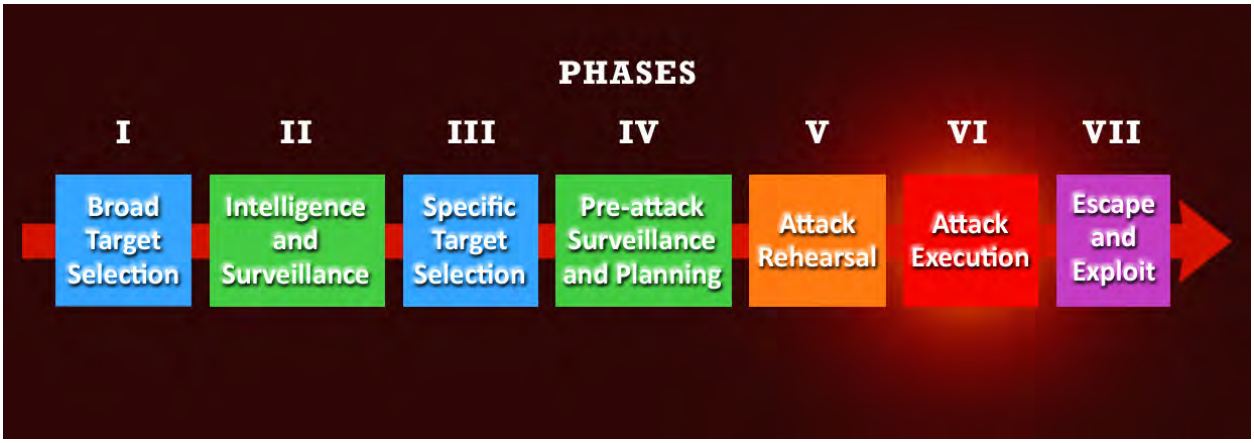


Figure 1, Terrorist Planning Cycle

Throughout the cycle, terrorists gather information on potential targets, determine the likelihood of a successful attack, make decisions on tactics, commit available resources, establish execution timelines, and train and rehearse for the operation. At any time throughout the cycle, attack planning can be halted or accelerated based on information gathered or changes in the group's intentions. Army forces can influence the terrorist planning cycle throughout all phases. However, the greatest likelihood of identifying and influencing terrorist activities is during the intelligence and surveillance phases (Phases II and IV) when threat force actions are more likely observable.

COMMUNITY AWARENESS

Given the persistent threat of terrorism, active community awareness programs (such as iWATCH Army and iSALUTE) are vital to the protection of Army installations, standalone facilities (SAFs), and operational units.

iWATCH Army is a form of neighborhood watch tailored specifically toward efforts to detect suspicious activity related to terrorist activities. iWATCH Army encourages and empowers the Army community to identify and report suspicious activity or behavior so law enforcement can investigate further to determine the actual risk and associated actions. The passive element of iWATCH Army is individual community members (Soldiers, civilians, family members, and contractors) with situational awareness of their surroundings. The active element of iWATCH Army involves individuals taking action to report suspicious behavior or activities to military police or local law enforcement for investigation. At the local installation, SAF, and unit level, community members report suspicious activity to the military police or local law enforcement using either 911 or locally established iWATCH telephone numbers.

iSALUTE was initially launched in response to the Fort Hood shootings as a tool to report insider threats to the U.S. Army. The term "iSALUTE" was coined from the Army's "SALUTE" report that Soldiers submit in the field when in contact with the enemy. iSALUTE allows U.S. Army personnel to submit a SALUTE report "inside the wire" and notify U.S. Army Counterintelligence (CI) of the threat. U.S. Army CI can then take proactive measures to investigate and mitigate the threat to U.S. Army personnel and equities. iSALUTE, as an online reporting tool, is analogous to 1-800-CALL-SPY and is an official reporting mechanism as taught in annual Threat Awareness and Reporting Program (TARP) training.

Report by telephone

- 1-800-CALL-SPY (1-800-225-5779) [continental U.S.]
- +49 (0) 611 143 537 2176 / DSN 314-537-2176 [Europe]
- 0505-723-3299/DSN 723-3299 [Korea]

Currently, iSALUTE exists as two separate versions, one on AKO and one on the public INSCOM website (https://www.inscom.army.mil). The public version was created so Army personnel can submit a report anywhere and anytime without relying on AKO, which requires a Common Access Card (CAC). The public version can be accessed from any major U.S. Army website from the iSALUTE link. iSALUTE provides a means for U.S. Army military, civilian, and contractor personnel to report threat-related incidents or terrorist threats directly to U.S. Army CI (source: AR 381-12, Military Intelligence: TARP).

To support information sharing between Army CI and Army criminal investigations, a U.S. Army Criminal Investigation Command (USACIDC) Special Agent is assigned to the Army CI Coordinating Authority to assist in the identification and transfer of incidents of Army criminal matters under the purview of USACIDC.

INTRODUCTION TO EGUARDIAN

Department of Defense Instruction 2000.26, Suspicious Activity Reporting (1 November 2011), designated eGuardian as the DoD system for suspicious activity reporting by DoD law enforcement agencies and activities. The eGuardian system is a sensitive, but unclassified, reporting system developed, owned, and operated by the Federal Bureau of Investigation (FBI). eGuardian allows the FBI to collect suspicious activity threat information and evaluate the information to determine whether there is a nexus to terrorism. eGuardian is restricted to duly authorized law enforcement agencies.

INDICATORS OF SUSPICIOUS ACTIVITY

Ensuring that all members of the Army community are educated about what to look for in terms of suspicious activity and how and what to report represents the foundation of effective AT awareness. The list below offers a starting point of commonly agreed-upon indicators. In reality, the factors associated with "what is suspicious" can involve things that are simply out of the ordinary for the environment.

Possible indicators of suspicious activity or high-risk behavior

- 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.

Reports of suspicious activity must undergo analysis to determine whether the activity or behavior relates to other events, associations, patterns, or trends, in an attempt to assess the overall risk and to inform decisions associated with protective measures.

THREAT INFORMATION SHARING

Threat information stemming from local reporting is investigated by law enforcement and other appropriate agencies (such as Army Counterintelligence) but may rise to the level of importance where it becomes an item of discussion at the installation or SAF threat working group (TWG). **Figure 2** provides a general flowchart for threat information. Threat information reviewed by the TWG should consider the need to further disseminate the information up, down, and laterally across the organization. Threat information which warrants tracking is typically shared with the next higher headquarters while disseminated to the tenant units and activities. The TWG, as a body which supports the overall AT plan, is responsible for reporting high-priority threat information to the AT Working Group and AT Executive Committee for situational awareness and as appropriate to inform decision-making. Commands should tailor their threat information flow as appropriate to their specific needs while documenting the process within their AT plan.

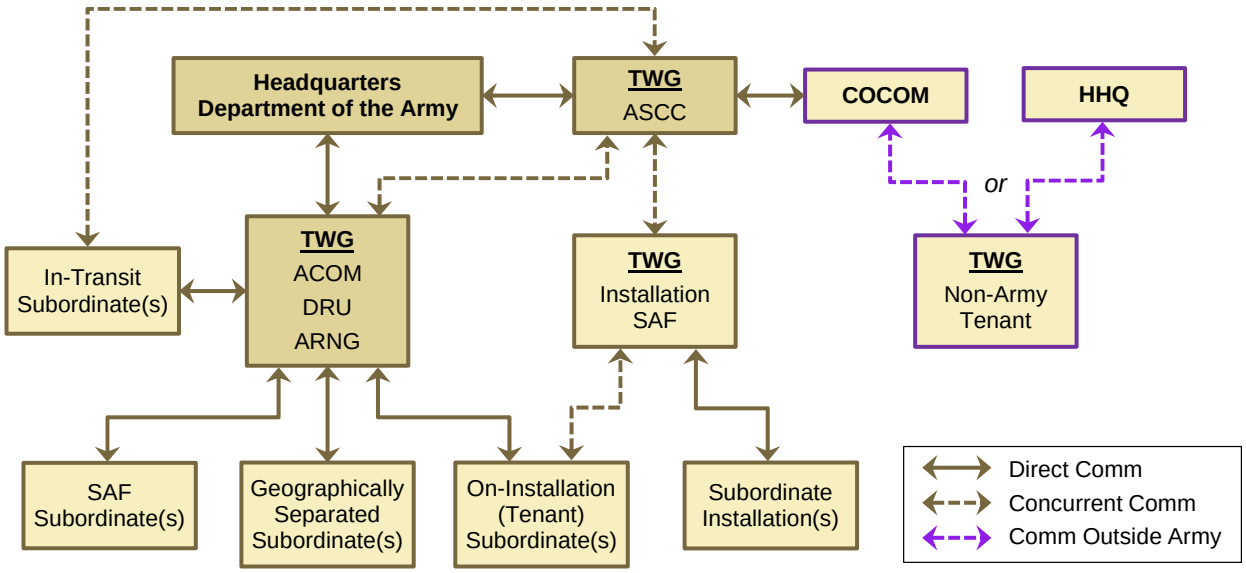


Figure 2, Threat Information Flow

On any given day it's possible an installation or SAF may review multiple threats which it is analyzing and sharing throughout the AT and broader protection community. There may be multiple TWGs working to assess the threat and to determine appropriate recommendations for the commander.

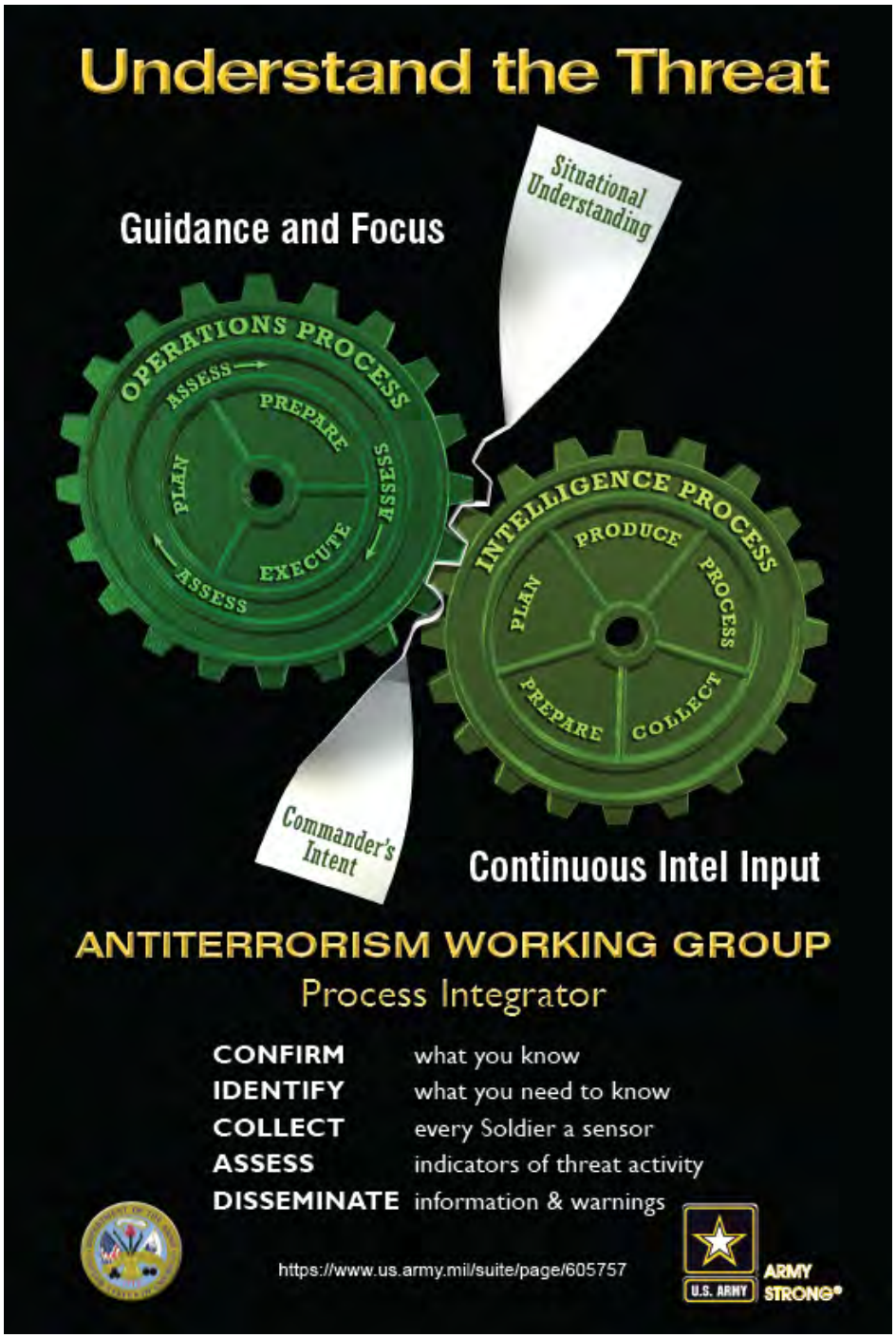
EGUARDIAN THREAT INFORMATION

All eGuardian reports developed within the Army go directly to the USACIDC Command Intelligence Operations Center (CIOC) (eGuardian Section) for review, quality control, and release into the eGuardian system. Although all eGuardian reports move up into Guardian (where the FBI does all the assessment work), USACIDC's CIOC provides a copy of the eGuardian report to the Army Threat Integration Center, the National Joint Terrorism Task Force, JC3, and the other military criminal investigative organizations as appropriate. eGuardian is a means to report raw information into the system to allow the servicing Joint Terrorism Task Force (and/or criminal investigation division or Military Police investigator) to assess the information to determine whether there is a possible (or actual) nexus to terrorism. The installation Provost Marshal Office, criminal investigation division office, or other authorized reporting element (e.g., ACOE or AMC) enters the report into eGuardian.

Threat information within eGuardian is readily available for analysis by Army law enforcement personnel at every level of command. In addition, the USACIDC CIOC and the Office of the Provost Marshal General's Army Threat Integration Center have access to eGuardian for threat fusion.

SUMMARY

Threat information is a critical element of AT risk assessment and a principal driver of threat response activities on an installation or SAF. Understanding the flow of threat information from initial report through the TWG and into eGuardian is vital to synchronizing information across the AT and protection communities.



Always Ready, Always Alert

Because someone is depending on you

Army Strong℠