Insider Threats in Partnering Environments

A Guide for Military Leaders (JUNE 2011)

THINK
ADAPT
ANTICIPATE

This guide assists in three areas. First, it aides military leaders and all personnel to be aware of the indicators associated with insider threat activity while serving in a partnering environment. Second, this guide informs commanders and other leaders by giving them options on how to deal with insider threat activities. This guide is not all encompassing so there are other options a commander has dependent on their operating environment. Lastly, this guide is meant to generate open dialogue between coalition partners and partner nation personnel. Partnering in itself is a sensitive mission and only by creating trust and having an open dialogue with all forces will the mission be accomplished.

OBSERVABLE INDICATORS

Early indicators of violent behavior are often displayed before an insider attack occurs. The indicators below can help identify a threat before violence is committed. This and the other lists gathered in this guide are not to be used as a check list. It is possible that only one or two indicators could be used to identify a threat. It should also be noted that it is poss ble for only one or two indicators to be spotted by an outsider. Because of this, it is vitally important that you create bonds of trust and become comrades with partners.

OBSERVE
Poss ble Threat

→

FLAG
Prior to Violent Activity

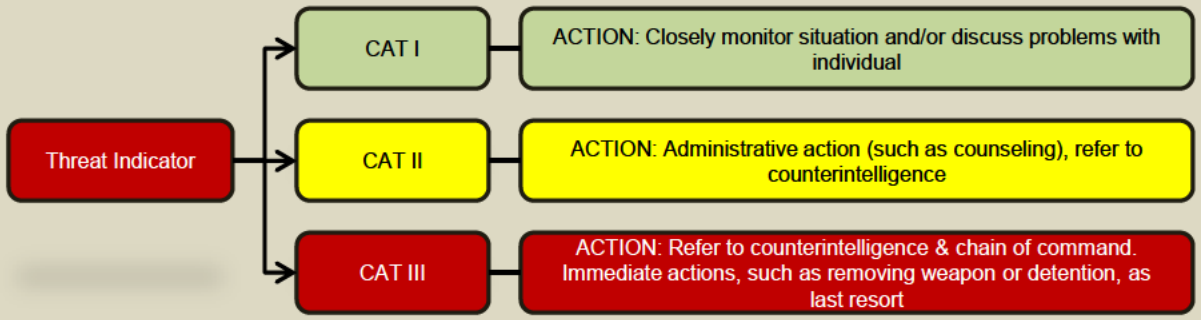
Indicators that should be observed for the subject's predisposition to become a threat.

Actions conducted by the subject that would indicate violent or terroristic planning

Category I Indicators
- Complains about other nations or religions
- Advocates violence beyond what is the accepted norm
- Abrupt behavioral shift
- Desires control
- Socially withdraws in some occasions
- Appears frustrated with partnered nations
- Experiences personal crisis
- Demonizes others
- Lacks positive identity with unit or country
- Reclusive
- Strange Habits
- Peculiar Discussions

Category II Indicators
- Verbally defends radical groups and/or ideologies
- Speaks about seeking revenge
- Associates with persons that have extremist beliefs
- Exhibits intolerance
- Personally connected to a grievance
- Cuts ties with unit, family, or friends
- Isolates self from unit members
- Intense ideological rhetoric
- Attempts to recruit others
- Choice of questionable reading materials in personal areas

Category III Indicators
- Advocates violence as a solution to problems
- Shows a sudden shift from "upset" to normal
- Takes suspicious travel or unauthorized absences
- Stores or collects ammunition or other items that could be used to injure or kill multiple personnel
- Verbal hatred of partner nation or individual from partner nation
- Exhibits sudden interest in partner nation headquarters or individual living quarters
- Makes threatening gestures or verbal threats

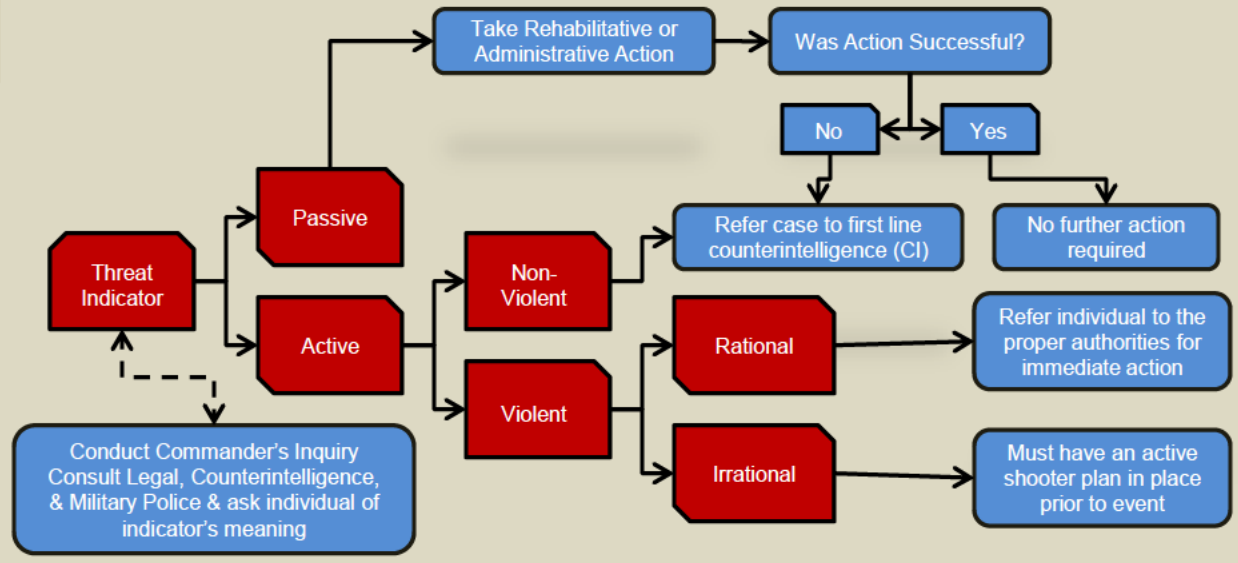


Some options used by the commander would irrevocably damage relationships with partner nation or coalition partners because of the loss of face or humiliation that occurs in the eyes of their peers. Ensure that the option chosen is the appropriate option for the situation.

EVERY SOLDIER IS A SENSOR

INDICATOR DECISION MATRIX

The decision support matrix is a guide for leaders to use if faced with an insider threat situation. This guide is not all encompassing and might not be applicable in all situations.



FORCE PROTECTION DECISION MATRIX

Criteria	Level	Recommended Actions
➢ Successfully completes a force protection (FP) screening ➢ No connections to any insurgent, terrorist, or extremist group and/or personalities ➢ No reporting showing derogatory information ➢ No large debts identified (more than $100 USD) ➢ Has a requirement for such access	POTENTIAL	Restricted Access / Can be unescorted
➢ Previous violations of installation policies / rules ➢ Has not been screened by FP personnel ➢ Suspected of corruption or illegal activity ➢ Uncorroborated or one-time reporting ➢ Family members identified as supporting illegal groups ➢ Failed vetting criteria used for maintaining or requesting access	MODERATE	Restricted Access / Should be escorted
➢ Theft or smuggling items on/off installation ➢ Efforts to access sensitive operational information ➢ Voices support or approval of insurgent, terrorist, or extremist groups ➢ Family members actively participating in illegal groups ➢ Selling / distributing drugs to installation personnel	HIGH	➢ Recommendation for firing, Biometrics Watchlist addition ➢ Pass REL dossier to host nation and coalition forces authority
➢ Family members are known insurgent, terrorist, or extremist group personnel ➢ Foreign intelligence agent or acknowledgement of foreign intelligence agent connections ➢ Latent fingerprints found on an object related to illegal groups ➢ Communicating information to third parties ➢ Reporting corroborated through intelligence	EXTREME	➢ Immediate removal, Biometrics Watchlist addition ➢ Possible Detention ➢ Pass REL dossier to host nation and coalition forces authority

Insider Threat Terms

- **Co-Opt:** voluntary or involuntary recruitment of existing member of an organization to work for an outside organization in order to conduct intelligence collection, subversion, sabotage, or violence
- **Infiltration:** insurgent, terrorist, or extremist group that places individuals into the security forces for the purposes of intelligence collection or violence
- **Grievance Based Action:** activities conducted in response to a wrong (perceived or real)perpetrated by the partnered individual, unit, or country. Not necessarily associated with extremist ideology but action could be used as extremist propaganda. These individuals are more suscept ble to co-opting.
  - **Grievance Based Homicide:** A subset of Grievance Based Action where an individual murders as a result of a perceived or real wrong.
- **Passive:** someone who is aware of insider activity or threat but whose inactivity allows the action to continue
- **Active:** willing to provide information or perform actions; may be violent or non-violent
  - **Violent:** active insiders who use force; they may act rationally or irrationally
    - **Rational:** well thought out, proportionate, violent course of action; possibly resulting in avoidance of capture
    - **Irrational:** disproportionate use of force often unplanned, emotional, and could involve collateral damage
  - **Non-Violent:** active insiders who are willing to provide information or conduct subversion, sabotage, and will conceal their actions
- **Radicalization:** the process by which an individual, group, or mass of people undergoes a transformation from participating in the political process via a legal means to the use, or support of, violence for political purposes
- **Extremist:** individuals who openly express their religious, political, or ideological views through violence or a call for violence
- **Mimicking:** a tactic used by the threat to gain access to personnel or facilities, normally off limits, by impersonating official personnel or soldiers (not addressed on this TRG)

Vetting Requirements

- Biometrics Screening
- Background Check
- Letter of Endorsement from community leader or already vetted personnel
  - Letter includes endorser's contact information to include phone number and email address if applicable
- Counterintelligence Interview
- Intelligence Reporting Check
- Emergency contact information
  - Includes phone number, email address and/or any other means of communication

VETTING IS AN ONGOING PROCESS

Risk Factors

- Emotional Vulnerability
- Dissatisfaction with lack of accepted conflict resolution
- Personal connection to a grievance
- Positive view of violence
- Perceived benefit of political violence
- Social Networks (tech and non tech)
- In group de-legitimization of the out-group
- Placement, Access, and Capability
- External Support
- Perceived Threat
- Conflict
- Humiliation or loss of honor
- Competition
- Social Alienation
- Quid Pro Quo (services or items wanted or needed by an individual given in exchange for information or action)
- Disproportionate financial risks
- Susceptible to blackmail
- Civilian Casualty (CIVCAS) situations
- Highly emotional
- Unfair treatment or equipment differences

Proactive Measures & Strategies

- Honesty assessment: initial and ongoing assessments of an individual's integrity, honesty, and reliability. These checks help identify motivational factors such as:
  - Greed
  - Financial factors
  - Ideological interests
  - Psychological factors
  - Desire for revenge
  - Physical dependency (drugs/ alcohol)
  - Other factors by which an individual could be coerced
- Examine personal viewpoints in light of values and loyalties to unit
- Reject affiliation with any extremist organization
- Encourage others (peers) to avoid extremist affiliations and views
- Report specific indicators to the chain of command
- Seek clarification from chain of command on "hot" topics, current issues, and current policies

Cultural Awareness

- DO NOT use derogatory terms in any language (even in friendly conversation)
- DO NOT slander host nation or coalition partners (even if only jokingly)
- DO NOT physically harm host nation or coalition partners (except in self defense)
- DO NOT put down or slander any religion
- ALWAYS be courteous and thankful for host nation and coalition partner hospitality

Preventive Tools

- Use of command climate type surveys and periodic sensing sessions
- Health and Welfare Inspections
- Conduct random sweeps of installation to identify unauthorized personnel (Insider Threat Surge / Clean Sweep Operations)
- Command visits to living quarters
- Use of counseling as a proactive course of action
- Develop workforce standards that mitigate risk, including hiring practices, security requirements, management practices for problem employees, disciplinary procedures, and grievance resolution
- Resources provided to employees in a crisis
- Develop training for reporting suspicious and aberrant behavior
- Educate partners on how to identify observable indicators and assist in developing mechanisms to allow reporting internally and to other coalition partners
- Access control procedures and compartmentalization of critical information, activities, and physical areas
- Educate members on poss ble sanctions (disciplinary actions and prosecution)
- Educate soldiers regarding the cultural differences by allowing the host nation to give cultural courses
- Establish confidential reporting procedures for threat indicators
- Use organic assets to collect information where there is a lack of Counterintelligence (CI) support (Every Soldier is a Sensor)
- Identify key personnel within the command structure that will carry handguns that are loaded at all times
- Obtain phone numbers and email addresses for host nation and other partners so that they could be reached and accounted for in an insider threat situation
- Random loaded weapon checks of all installation personnel

Increased Force Protection Criteria

- Civilian Casualty (CIVCAS) Event
  - Witnessing or hearing about civilian casualties could create a psychological hardship on host nation and coalition personnel. Giving host nation partners time to themselves (separation) as a cool off period is vital to mitigating a Grievance Based Action.
- Political Speeches
  - Political speeches from host nation leadership could negatively impact the mission. Have a plan in place to discuss the key points of the speech with partners and assure them we are in the fight together.
- Host Nation or Coalition Casualties
  - Losing a comrade in arms is a hard event and could lead to finger pointing or accusations of wrong doing; especially if the event was caused because of an equipment disparity. (Example: "I drive an unarmored vehicle and you drive an armored vehicle."). Assure partners that there will be an attempt to fix the problem and that any difference is not intentional.
- Global Events
  - With globalization information reaches every part of the world rapidly. If a religion is dishonored in one part of the world it is only a matter of time before it reaches the host nation or coalition partner's ears. Because of this, leadership should be prepared, again, to talk about the issues and show that the actions of some are not the actions of all.

References and URLs

SIPRNET SITES

- **Army Counterintelligence Center:** http://acic.north-inscom.army.smil.mil/ho01.asp
- **902d MI Group Insider Threat:** http://acicportal.north-inscom.army.smil.mil/cira/default.aspx
- **ANSF Insider Threat (Intellipedia):** http://www.intelink.sgov.gov/wiki/ANSF_Insider_Threat
- **Afghanistan Insider Threat:** http://www.afghan.centcom.smil.mil/intel/cj2x/ciit/default.aspx
- **Iraq Insider Threat:** http://cj2.s-iraq.centcom.smil.mil/CJ2X/Pages/default.aspx
- **USAREUR Threat Awareness and Reporting System (TARP):** http://intel.eur.aep.army.smil.mil/Ops/G2X/CI/saeda/default.aspx

PRODUCTS

- The Insider Threat: A Glimpse of the Problem, Challenges, and Countermeasures (U//FOUO) (Air Force Office of Special Investigations)
- Common Sense Guide to Prevention and Detection of Insider Threats (US-CERT)
- CJTF-101 Task Force Counterintelligence Coordinating Authority: Countering the Insider Threat (SECRET//REL ISAF NATO)

Helpful Hints

- Rapport
  - Establish a baseline attitude and demeanor for individuals
  - Show that you are a fellow soldier by your actions and speech
  - Treat individuals with respect
- Protect
  - Cipher lock and control access to critical buildings
  - Have roving guards conduct honesty checks on all individuals with weapons to ensure they are not loaded (US and Partner Nations)
- Screen
  - Enroll all personnel into biometrics entering coalition bases
  - Secure mobile phones at entry control points or at designated areas
- Report all suspicious activity

REPORT ALL SUSPICIOUS ACTIVITY