CHAPTER 6
INTELLIGENCE AND ELECTRONIC WARFARE SUPPORT TO COMBATTING TERRORISM

This chapter provides TTP needed to conduct the missions and functions of the intelligence disciplines to combat terrorism. It also addresses CI support to force protection in combatting terrorism.

Terrorism is generally described as the calculated use of violence, or the threat of violence, to inculcate fear intended to coerce or intimidate governments or societies in the pursuit of goals that are political, religious, or ideological. This is done through intimidation, coercion, or instilling fear. Terrorism involves a criminal act that is often symbolic in nature and intended to influence an audience beyond the immediate victims.

HUMAN INTELLIGENCE

In combatting terrorism, HUMINT is the first line of defense. Primary objectives are deterring, detecting, and preventing terrorist acts. The collection and development of HUMINT information on the terrorist threat is critical. HUMINT sources provide valuable information on terrorist organizations, capabilities, tactics, and targets. HUMINT collection operations include document exploitation, interrogations, and liaison.

Usable information can come from a variety of HUMINT sources including open sources, LEA, government intelligence agencies, and informal local contacts. These need to be accessed and exploited by the installation intelligence officer or combatting terrorism officer.

OPEN INFORMATION SOURCES

This information is publicly available, often overlooked, and reliable. Local and national news media and government and private sector publications are excellent open sources on terrorism. Also, terrorist groups, and their affiliates, may publish a variety of manuals, pamphlets, and newsletters that reveal their objectives, tactics, and possible targets. Information on specific groups and individuals must be collected and maintained in accordance with AR 381-10.

CRIMINAL INFORMATION SOURCES

Both military and civil LEA collect criminal information. Criminal information can be a valuable source of intelligence on terrorists. LEAs maintain informants and informant nets to collect intelligence on criminal activities. They can also provide information concerning terrorist plans, capabilities, recruitment, and targets.

Government Intelligence Agencies

Military and governmental intelligence and investigative agencies maintain extensive terrorist threat data. Intelligence threat analysis centers (ITACs) produce MDCI and terrorist threat summaries. Periodic regional threat packets are available from the local US Army Intelligence and Security Command (INSCOM) representative. The US Air Force Office of Special Investigations (OSI), DIA and CIA maintain comprehensive terrorist data bases, which can be accessed.

Intelligence officers need to establish routine liaison with the CI covering agents who support their organization. These individuals are a good source for obtaining terrorist information from local US military and governmental intelligence agencies. They also can assist in obtaining information from national level assets. CI personnel overseas can obtain terrorist data from HN intelligence and security agencies.

INFORMAL LOCAL SOURCES

Other valuable sources of information are individual soldiers, family members, or civilian employees. When approached and made aware of the potential terrorist threat, they can become valuable sources of information. These informal sources provide information on unusual or suspicious activities in their area.
You also need to ensure that the reporting of terrorist-related indicators is stressed during periodic terrorist threat briefings and SAEDA training.

Additionally, family members and employees need to be encouraged to report useful information through an active crime prevention program.

**IMAGERY INTELLIGENCE**

Imagery assets can provide timely information to operational units once terrorist activities have been initiated. Indeed, optical imagery or prints of terrorist training facilities can be studied to learn how a particular terrorist organization trains and operates. Facilities such as swimming pools (frogmen, underwater training), towers (airborne training), firing ranges, and physical training areas are some indicators used by the IAs to determine the terrorist group’s operating characteristics.

The initial identification of terrorist training facilities is usually made by IAs at the national level. However, units involved in combating terrorism should have on file imagery or prints of targets for reference. (See Appendix H.)

**SIGNALS INTELLIGENCE**

EW and SIGINT provide a limited contribution to combating terrorism. From an offensive standpoint, ESM maybe possible during terrorist criminal acts such as sabotage and kidnappings. Due to the nature of terrorist groups, the use of ECM will be minimal.

Because today’s terrorists are well trained and well equipped, combating them is best done before the fact, not after. The way to do this is to take all countermeasures possible. The proper use of ECCM will go a long way in deterring terrorist actions. Make sure you—

- Secure your equipment. Stolen equipment gives added capabilities to terrorist groups. If weapons and communications gear are discovered missing, make every effort to recover them. Stolen weapons have been used in actions against US forces and installations. Likewise, stolen communications equipment can be used by terrorists to target our people by conducting radio intercept operations.

- Use the telephone carefully. Today’s terrorists have the capability and know-how to tap telephone systems, particularly overseas. Use a secure telephone to discuss classified information, visiting dignitary itineraries, and key personnel travels. Do not try to talk around issues. If a secure means of communications is not available, find another way to conduct business or do not do it.

Above all, if you or your unit is involved in combating terrorism, remember that MI jurisdiction is limited by executive orders, federal laws, Army regulations, directives, international agreements, and SOFAS. One example of these is Title 18 of the US Code. Verify the legality of pending operations with the legal officer of the local MI brigade.

**COUNTERINTELLIGENCE**

MDCI support to combating terrorism focuses on protecting the force and is primarily preventive in nature. MDCI support ranges from strategic to echelons corps and below (ECB). This support is accomplished through the four functional areas of investigations, operations, collection, and analysis and production. MDCI support includes—

- Preparing and maintaining a threat database pertaining to terrorist and FIS multidiscipline intelligence collection capabilities (HUMINT, IMINT, and SIGINT).
- Preparing terrorist threat analysis.
- Providing MDCI threat evaluations of foreign intelligence and terrorist organizations.
- Alerting Army commanders to terrorist threats against their personnel, facilities, and activities.
- Assisting operations personnel in assessing vulnerabilities and recommending protective countermeasures.
- Investigating terrorist incidents for intelligence value.
- Conducting liaison with federal, state, and local agencies and HN federal, state, and local agencies,
to exchange information on terrorist and FIS activities.

- Conducting CI operations to include SAEDA briefings, investigating deliberate security violations, and providing security A&A.
- Conducting collection operations to include LLSO.

The senior CI officer will determine specific tasks that need to be performed in accordance with regulatory requirements and SOFAS with the HN. Appendix C describes the MDCI analytical process used in—

- Combatting terrorism.
- Terrorist assessments.
- Friendly force assessments.
- Countermeasures recommendations.
- Countermeasures evaluations.

The MDCI analyst needs to evaluate the supported command’s OPSEC program and make recommendations to improve force protection measures. Force protection needs to be tailored to fit each installation or separately deployed unit.