FIELD MANUAL
NO. 34-60

*FM 34-60
HEADQUARTERS
DEPARTMENT OF THE ARMY
Washington, DC, 3 October 1995

COUNTERINTELLIGENCE

TABLE OF CONTENTS

*This publication supersedes FM 34-60, 5 February 1990.

Page

PREFACE

This field manual (FM) provides guidance to commanders, counterintelligence (CI) agents, and analysts. The first four chapters provide information to the commander and staff while the remainder provides the tactics, techniques, and procedures (TTP) required to aggressively identify, neutralize, and exploit foreign intelligence attempts to conduct operations against the United States (US) Army.

CI supports Army operations by providing a clear picture of the threat to commands at all echelons and actions required to protect the force from exploitation by foreign intelligence. CI operations include conducting investigations, offensive and defensive operations, security and vulnerability analyses, and intelligence collection in peace and at all levels of conflict to support command needs.

CI supports the total intelligence process by focusing on foreign intelligence collection efforts. CI is designed to provide commanders the enemy intelligence collection situation and targeting information in order to counter foreign intelligence service (FIS) activities. CI is an integral part of the US Army's all-source intelligence capability.

By its nature, CI is a multidiscipline effort that includes counter-human intelligence (C-HUMINT), counter-signals intelligence (C-SIGINT), and counter-imagery intelligence (C-IMINT) designed to counter foreign all-source collection. The CI force in conjunction with other intelligence assets must have the capability to detect all aspects of intelligence collection and related activities that pose a threat to the security of Army operations, personnel, and materiel. Through its database (friendly and adversary) and analytical capability, CI provides sound recommendations, which if implemented, will result in the denial of information to the threat.

It should be noted that any decision regarding the implementation of CI recommendations aimed at denying collection opportunities to the adversary is a command decision. The commander may decide to accept the risk of enemy collection in favor of time, resources, or other higher priority considerations. At that point, the CI mission is considered to be successful because it is a tool of the commander.

This manual is designed for use by commanders and their staffs; all military intelligence (Ml) commanders, their staffs, and trainers; and Ml personnel at all echelons. It applies equally to the Active Army, United States Army Reserve (USAR), and Army National Guard (ARNG). It is also intended for commanders and staffs of joint and combined commands, United States Naval and Marine Forces, units of the US Air Force, and the military forces of allied countries.

Provisions of this manual are subject to international Standardization Agreements (STANAGs) 2363 and 2844 (Edition Two). When amendment, revision, or cancellation of this publication affects or violates the international agreements concerned, the preparing agency will take appropriate reconciliation action through international standardization channels.

The proponent of this publication is the United States Army Intelligence Center and Fort Huachuca. Send comments and recommendations on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Commander, US Army Intelligence Center and Fort Huachuca, ATTN: ATZS-TDL-D, Fort Huachuca, AZ 85613-6000.

Unless this publication states otherwise, masculine nouns and pronouns do not refer exclusively to men.

This chapter implements STANAG 2844 (Edition Two)

Chapter 1

MISSION AND STRUCTURE

GENERAL

Threat intelligence services have the capability to conduct continuous collection against the US Army during peacetime, operations other than war (OOTW), and during war itself. The intelligence that results from these operations provides a significant advantage to threat forces, and could easily result in increased US casualties on the battlefield. Fortunately, there are many actions we can take to counter threat intelligence efforts and to provide force protection to all US Army units.

The most dramatic of these actions are designed to neutralize enemy collection. These actions include—

- Using field artillery to destroy ground-based enemy signals intelligence (SIGINT) collectors.
- Conducting sophisticated C-HUMINT operations in a foreign city long before overt hostilities commence.
- Employing direct fire weapon systems to destroy enemy reconnaissance. Brigades conducting defensive operations at the National Training Center often commit a tank-infantry company team to provide counterreconnaissance, intelligence, surveillance, and target acquisition (C-RISTA) protection.

While not as flashy, routine security procedures provide crucial force protection. These procedures include but are not limited to—

- Personnel security, to include background investigations, will ensure all personnel who have access to sensitive or classified information will fully protect it.
- Information security, particularly in regard to handling classified and compartmented information, will be a challenging field in the future considering the ease with which information can be copied and transmitted in an increasingly automated Army.