Army Regulation 525–21

Military Operations

Tactical Deception (TAC–D) Policy (Including Camouflage, Countersurveillance, and Concealment)

Headquarters
Department of the Army
Washington, DC
15 June 1982

UNCLASSIFIED

SUMMARY of CHANGE

AR 525–21
Tactical Deception (TAC–D) Policy (Including Camouflage, Countersurveillance, and Concealment)

This regulation--

- Sets forth the Army’s tactical deception (TAC-D) policy;

- Describes the role of TAC-D in combat operations, and identifies objectives and assigns responsibilities for TAC-D.

Headquarters
Department of the Army
Washington, DC
15 June 1982

Army Regulation 525–21

Effective 15 July 1982

Military Operations

Tactical Deception (TAC–D) Policy (Including Camouflage, Countersurveillance, and Concealment)

By Order of the Secretary of the Army:

E. C. MEYER
General, United States Army
Chief of Staff

Official:

ROBERT M. JOYCE
Brigadier General, United States Army
The Adjutant General

History. This publication has been organized to make it compatible with the Army electronic publishing database. No content has been changed.

Summary. This regulation provides instructions for achieving the tactical deception posture needed to accomplish assigned operational missions effectively in all elements of the US Army.

Applicability. This regulation applies to the Active Army, the Army National Guard (ARNG), and the US Army Reserve (USAR).

Proponent and exception authority. The proponent agency for this regulation is the Office of the Deputy Chief of Staff for Operations and Plans.

Army management control process. This regulation contains management control provisions but does not identify key management controls that must be evaluated.

Supplementation. Local limited supplementation of this regulation is permitted but is not required. If supplements are issued, HQDA agencies and major Army commands will furnish one copy of each to HQDA (DAMO-RQI), WASH DC 20310; other commands will furnish one copy of each to the next higher headquarters.

Interim changes. Interim changes to this regulation are not official unless they are authenticated by The Adjutant General. Users will destroy interim changes on their expiration dates unless sooner superseded or rescinded.

Suggested Improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) direct to HQDA (DAMO-RQI), WASH DC 20310.

Distribution. *Active Army, ARNG, USAR:* To be distributed in accordance with DA Form 12-9A requirements for AR, Military Operations—C

Contents (Listed by paragraph and page number)

UNCLASSIFIED

RESERVED

1. Purpose.

This regulation sets forth the Army's tactical deception (TAC–D) policy; it also describes the role of TAC–D in combat operations, and identifies objectives and assigns responsibilities for TAC–D.

2. Applicability.

This regulation applies to the Active Army, the Army National Guard (ARNG), and the US Army Reserve (USAR).

3. References.

Related publications are listed in appendix A.

4. Explanation of terms.

Special terms used in this regulation are explained in the glossary.

5. Responsibilities.

a. Deputy Chief of Staff for Operations and Plans (DCSOPS). The DCSOPS will—

(1) Supervise and coordinate the Army's TAC–D activities.

(2) Monitor the TAC–D force readiness and determine operational capabilities of Army forces to accomplish assigned missions under real or assumed conditions.

(3) Supervise the integration of TAC–D into Army plans, operations, and unit training.

(4) Provide for integration of TAC–D systems into Army forces.

(5) Develop Army TAC–D policy, programs, and force requirements for units of the Active Army, ARNG, and USAR.

(6) Provide Army Staff supervision of planning, execution, and evaluation of TAC–D activities in field training exercises.

(7) Validate, coordinate, and approve materiel requirements documentation and establish priorities in support of TAC–D programs.

(8) Provide Army Staff supervision of operational testing of TAC–D equipment, systems, and organizations.

(9) Insure that TAC–D is incorporated in Army doctrine, concepts, materiel development, and training.

(10) Assess TAC–D interoperability with the other Military Services and Allies; make recommendations for improvements.

(11) Coordinate TAC–D matters with the other Military Services and Allies as appropriate.

(12) Review TAC–D operational and organizational concepts, doctrine, and unit training.

(13) Develop policies and programs for individual TAC–D training within general subjects programs of instruction (POI).

(14) Provide input to Army personnel and personnel management programs.

b. Deputy Chief of Staff for Research, Development, and Acquisition (DCSRDA). The DCSRDA will—

(1) Conduct research, development, test, and evaluation (RDTE) of specialized materiel required to support TAC–D operations.

(2) Conduct acquisition and life-cycle management of TAC–D materiel.

(3) Plan and coordinate the development or procurement of systems for testing and training in support of TAC–D programs.

c. Deputy Chief of Staff for Personnel (DCSPER). The DCSPER is responsible for manpower and personnel management associated with TAC–D activities.

d. Deputy Chief of Staff for Logistics (DCSLOG). The DCSLOG will provide—

(1) Logistic support of TAC–D materiel within DCSLOG-assigned functions. This includes the application of the Integrated Logistic Support (ILS) Program during the materiel acquisition process.

(2) Continuous logistic support for fielded TAC–D materiel and test equipment.

e. Assistant Chief of Staff for Intelligence (ACSI). The ACSI will—

(1) Provide intelligence support to TAC–D programs.

(2) Provide surveillance and target acquisition threat, and information on enemy intelligence gathering capabilities.

(3) Monitor and coordinate the intelligence aspects of threat TAC–D.

f. Commanding General, US Army Operational Test and Evaluation Agency (OTEA). The CG–OTEA will—

(1) Exercise responsibility for operational testing of TAC–D related systems in a surveillance, target acquisition, and intelligence gathering threat environment.

(2) Conduct operational tests on assigned major and category I non-major TAC–D-related systems in an environment that represents the hostile surveillance, target acquisition, and intelligence gathering threat. This will be done in accordance with user-specified issues.

(3) Review plans and other test documents prepared by designated testers for category 2-4 nonmajor systems. Insure

system vulnerabilities to hostile surveillance, target acquisition, and intelligence-gathering capabilities are appropriately addressed.

g. Commanding General, US Army Training and Doctrine Command (CG, TRADOC.) The CG, TRADOC will—

(1) Develop and test TAC–D organizational and operational plans at doctrine for use of TACD in support of Army operations at Corps echelon and below.

(2) Recommend science and technology objective (STO) for TAC–D to HQDA.

(3) Prepare and provide recommendations on establishing, revising, or eliminating materiel requirements documents for Army-wide TAC–D operations.

(4) Program for, and conduct, troop TAC–D tests, as required.

(5) Evaluate the effectiveness of TAC–D equipment in the field throughout its life cycle; recommend improvements in this equipment.

(6) Direct and supervise the preparation of training literature for TAC–D equipment; direct and supervise the training of personnel in the use, operation, and maintenance of TAC–D materiel.

(7) Integrate TAC–D doctrine and concepts into the curriculum of TRADOC schools.

(8) Integrate potentially hostile surveillance, target acquisition, and intelligence-gathering threat into combat developments and training activities.

(9) Recommend establishment, revision, or elimination of training device requirements (TDR) for TAC–D training.

(10) Include TAC–D in Army Training and Evaluation Program (ARTEPS).

h. Commanding General, US Army Materiel Development and Readiness Command (CG, DARCOM). The CG, DARCOM will—

(1) Perform the functions of TAC–D materiel RDTE, procurement, storage, depot maintenance, and issue, as assigned by HQDA.

(2) Include logistical support of all TAC–D systems in the ILS Program.

(3) Prepare technical literature on operation and maintenance of TAC–D materiel in a hostile surveillance, target acquisition, and intelligence gathering environment.

(4) Conduct research into, and acquire basic knowledge of, techniques and tactics required for an effective TAC–D capability in appropriate Army systems.

(5) Incorporate maximum cost-effective countersurveillance features, and other defensive TAC–D features, into susceptible communications electronic (C-E) equipment and weapons; recommend trade-offs to the combat developer.

(6) Conduct developmental tests and studies on the susceptibility of Army systems to hostile surveillance target acquisition, and intelligence gathering activities.

(7) Provide support and assistance, as required, to other major Army commands in meeting their assigned TAC–D responsibilities.

(8) Develop and procure TAC–D systems for testing and training as required and when requested.

i. Commanding General, US Army Intelligence and Security Command (CG, INSCOM). The CG, INSCOM will—

(1) Support other MACOMs and activities during exercises, tests, experiments, and combat. This will include assistance in the assessment of the effectiveness of applied TAC–D concepts.

(2) Recommend changes or additions to TRADOC for TAC–D concepts, doctrine, and related matters at the Corps echelon and below.

(3) Participate in combat development studies, experiments, and tests of TAC–D organizational and operational concepts and doctrine, as requested by the CG, TRADOC.

(4) Provide advice and assistance to other MACOMs in determining their countersurveillance, target acquisition, and intelligence-gathering vulnerabilities in relation to enemy expected or observed intelligence operations.

(5) Recommend STO for TAC–D to TRADOC.

(6) Perform TAC–D RDTE and materiel acquisition functions assigned by HQDA.

(7) When requested, assist TRADOC in preparing and reviewing STOs and required operational capabilities (ROCs) for TAC–D systems and equipment to insure that signal security (SIGSEC) and operations security (OPSEC) requirements are adequate and realistic.

(8) Conduct other TAC–D and TAC–D–related missions, as assigned.

j. Commanding General, US Army Communications Command (CG, USACC). The CG, USACC will—

(1) Develop, test, and recommend to TRADOC organizational and operational concepts and doctrine pertaining to the use of TAC–D capabilities to support the following activities: Army Air Traffic Control Facilities, USACC-operated facilities at Corps echelon and below, and the Army portion of the Defense Communications System.

(2) Integrate hostile surveillance, target acquisition, and intelligence-gathering threat in combat development and training activities that will carry out the missions and functions of USACC.

(3) Prepare literature pertaining to the operation of mission peculiar equipment in the hostile surveillance, target acquisition, and intelligence-gathering environment.

(4) Assist DARCOM in determining the surveillance, target acquisition, and intelligence-gathering vulnerabilities of USACC systems.

(5) Conduct susceptibility and vulnerability tests and studies on mission peculiar equipment and systems, as appropriate.

k. Commanding General, US Army Forces Command (CG, FORSCOM) and Commanders of Army Tactical Commands. The CG, FORSCOM and Commanders of Army Tactical Commands will—

(1) Develop and maintain a capability to perform TAC–D functions to support operational plans; this will include electromagnetic cover and deception (EC&D).

(2) Train commanders, staff members, and communications and intelligence personnel to—

(a) Understand and detect hostile surveillance, target acquisition, and intelligence gathering capabilities.

(b) Plan and make decisions effectively for TAC–D support of operational and OPSEC plans.

(3) Exercise operational control over all TAC–D resources assigned to them.

(4) Maintain TAC–D readiness for Army forces assigned to them.

(5) Integrate TAC–D training into unit training programs, maneuvers, and exercises, as appropriate.

(6) Recommend to TRADOC changes or additions to TAC–D concepts, doctrine, tactics, or techniques that may result from evaluation of training given in (3) above.

(7) Designate a component on headquarters staffs to serve as the focal point for TAC–D matters.

(8) Identify operational and intelligence requirements, conduct appropriate test and evaluation activities, and procure equipment needed to reach required TAC–D posture, in consonance with other known requirements and priorities.

(9) Identify personnel requirements and qualifications for TAC–D activities; train and provide personnel to subordinate operational commands.

(10) Insure that command and control capabilities are adequate to support the planning and conducting of TAC–D activities.

(11) Maintain personnel security programs to protect against compromise of TAC–D plans, capabilities, and activities; provide guards and other defensive forces to carry out this protection.

6. Guidance.

The basic strategies of tactical commanders are to surprise the enemy, accomplish the assigned mission, and keep casualties at a minimum. Modern technology has provided hostile commanders with greatly expanded capabilities; they may more easily determine the dispositions, capabilities, and intentions of their opponents' units. This has increased the difficulty of friendly tactical commanders to execute their planned strategy.

a. The primary goal of TAC–D is to support tactical operations by improving chances of successfully executing the planned strategy of the tactical commanders. This will be done by minimizing the effectiveness of the hostile commanders' intelligence and battlefield information-gathering resources. In this way, tactical commanders can control and manage hostile commanders' perceptions of friendly capabilities and intentions.

b. TAC–D includes that portion of military deception that is—

(1) Planned and executed by combat, combat support, and combat service support elements at Corps echelon and below.

(2) Aimed at hostile elements collecting intelligence or information against these echelons.

c. TAC–D operations are also conducted to support the following command activities:

(1) OPSEC.

(2) Command, control, and communications (C^3) countermeasures (C^3CM).

(3) Electronics warfare (EW).

(4) Military deception.

(5) Inclusive functions of countersurveillance, camouflage, and concealment.

d. TAC–D operations must address all potential threats to avoid compromise, eliminate false security, and insure effectiveness. Enemy threats use visual, acoustic, electromagnetic, and olfactory methods. These threats and TAC–D actions, which can be used to counter them, are discussed below.

(1) Visual methods include ground or airborne observers using the human eye with or without visual aids such as binoculars and night vision devices, and ground and airborne photography. Camouflage and concealment can be effectively used against the hostile visual surveillance and target acquisition threat in all portions of the electromagnetic spectrum.

(2) Acoustic methods include ground or airborne observers using the human ear with or without aural aids such as amplifiers and acoustic signal analyses. Power amplifiers for broadcasting false battlefield sounds can be used against hostile acoustic sensors.

(3) Electromagnetic methods include the following:

(a) Battlefield surveillance, artillery target acquisition, and countermortar or counterbattery raiders.

(b) Intercept and direction-finding collection activities.

(c) Night vision devices.

(d) Infrared surveillance and target acquisition systems.

(e) Other systems or devices that use radiated electromagnetic energy.

(f) Activities using electro-optical equipment.

(4) Electronic countermeasures (ECM) can be effectively used against hostile radio receivers and active or passive sensors using electromagnetic energy. These include the following:

(a) Electronic jamming that degrades the effective use of radar and communications assets.

(b) Manipulative electronic deception (MED) activities that alter electromagnetic radiation's or procedures. These will eliminate tell-tale indicators of stereotypical characteristics that benefit enemy intelligence collection activities.

(c) Simulative electronic deception (SED) activities that disguise unit deployments by creating false radiation's from notional or actual units or weapon systems.

(d) Imitative electronic deception (IED) that intrudes on hostile electromagnetic sensors or command and control systems to present false data.

(e) Absorption, reflection, suppression, or enhancement devices or materials that can distort, disguise, or degrade hostile sensors, or create decoys for deception.

(5) Olfactory methods that use the sense of smell. TAC–D tactics such as dispersing of oil depots or creating dummy odors by scattering droplets can be effective against hostile olfactory sensors.

e. TAC–D is never performed as an end in itself; instead, it is used as an integral element of tactical operations or survivability activities.

f. Certain TAC–D activities may require specially trained and equipped units, but, in general, all Army combat, combat support, and combat service support units must be capable of exercising basic TAC–D functions.

7. Roles of TAC–D.

The two major roles of TAC–D are discussed below.

a. Achieve a level of competence among all Army elements that will enable them to defeat hostile surveillance, target acquisition, and intelligence-gathering activities on the battlefield. These will include radar intelligence (RADINT), human intelligence (HUMINT), signal intelligence (SIGINT), and imagery intelligence (IMINT). These activities seek to hide the real, which is the camouflage, counter surveillance, and concealment component of TAC–D.

b. Create false impressions about friendly deployments, capabilities, and intentions, achieving a condition advantageous to friendly forces. These activities seek to portray the false, which is the deception component of TAC–D.

8. Objectives.

TAC–D objectives are outlined below.

a. Maximize US Army capabilities to do the following:

(1) Prevent hostile military commanders from using their tactical surveillance, target acquisition, and intelligence-gathering assets effectively; this will mislead these hostile commanders by influencing their decision-making process.

(2) Influence hostile commanders' decisions by creating inaccurate perceptions of friendly combat deployments, capabilities, and intentions; this will improve the chances of accomplishing the mission and reducing casualties by achieving surprise.

(3) Deny hostile commanders intelligence and information so that their decisions are based on incomplete data.

b. Integrate TAC–D into military plans, operations, and exercises for maximum US and Allied military effectiveness.

c. Develop TAC–D capabilities that are interoperable, compatible, and mutually supportive in joint and combined operations.

d. Train or familiarize personnel at all levels with TAC–D activities, capabilities, and limitations.

e. Evaluate the effects of TAC–D on friendly and hostile surveillance, target acquisition, and intelligence-gathering activities.

9. Policy.

a. Commanders of MACOMs and component commands will develop capabilities at Corps echelons and below to use TAC–D during day-to-day operations, mobilization, periods of international tension, and war.

b. US Army tactical commanders will use TAC–D to maximize the effectiveness and maintain the security of US Army operations and exercises.

c. US Army TAC–D programs, tactics, and concepts will be coordinated with DOD components and Allied nations, when applicable.

d. US Army TAC–D procedures and materiel programs will—

(1) Respond to operational goals and objectives.

(2) Complement the effects of other weapon systems.

(3) Support effectively the combat efforts of the United States and its Allies.

e. Interoperability will be attained on a step-by-step basis; its focus will be to achieve a capability that meets joint and combined needs and individual US Army requirements.

f. Systems that may be affected by hostile surveillance or target acquisition will be tested in a representative environment; this environment will quantitatively portray the expected threat as realistically as practical.

g. Devices, systems, and materiel having TACD potential will be tested against capabilities that represent the expected threat.

h. Tests involving TAC–D equipment, materiel, and procedures will be protected by OPSEC measures against foreign intelligence collection.

i. TAC–D capabilities will be considered, and incorporated, when proper, into the following functions:

(1) US Army mission area analyses (MAA).

(2) Operational requirements documents.

(3) Mission element needs statements.

(4) Subsequent development, designs, and test of systems.

j. Incorporating TAC–D into operations will be a standing objective in all major Army exercises. TAC–D will be given priority over other exercise objectives during specified portions of the exercises; this will be done to evaluate the capability of US Army combat, combat support, and combat service support elements to perform both cover and deception in a hostile threat environment.

k. US Army intelligence elements will provide support to TAC–D planners and commanders at all echelons for planning and conducting TAC–D. These intelligence elements will assist in preparing scenarios that represent anticipated threats; they will provide analysis for assessing the effectiveness of TAC–D plans, tactics, and assets.

l. Protection of friendly C^3 and weapon systems from hostile surveillance, target acquisition, and intelligence gathering will be a command responsibility.

m. Responsibility will be shared by the proponent, developer, and user for eliminating or minimizing susceptibility to surveillance, target acquisition, and intelligence gathering of C^3 and electronics-dependent equipment under development.

n. TAC–D training will be addressed during Army Training and Evaluation Program (ARTEP) activities.

o. Because OPSEC is an essential element for effective TAC–D operations, TAC–D normally will be preceded by a threat and vulnerability analysis.

Appendix A
RELATED PUBLICATIONS

Section I
Required Publications
This section contains no entries.

Section II
Related Publications
A related publication is merely a source of additional information. The user does not have to read it to understand this regulation.

AR 70–1
(Army Research, Development, and Acquisition).

AR 70–10
(Test and Evaluation during Development and Acquisition of Materiel).

AR 105–1
(Telecommunications Management).

(C) AR 105–2
(Electronic Counter-Countermeasures (ECCM) Electronic Warfare Susceptibility and Vulnerability) (U).

AR 105–3
(Reporting Meaconing, Intrusion, Jamming, and Interference of Electromagnetic Systems).

AR 105–5
(Electromagnetic Cover and Deception (EC&D)).

AR 105–7
(Quick Reaction Capability (QRC) for Electronic Warfare).

AR 105–24
(Radio Frequency and Call Sign Assignments for US Army Communications-Electronics Activities).

(C) AR 105–87
(Electronic Warfare) (U).

AR 380–5
(Department of the Army Information Security Program).

(C) AR 380–10
(Department of the Army Policy for Disclosure of Military Information to Foreign Governments) (U).

AR 525–20
(Command, Control, and Communications Countermeasures (C^3CM) Policy).

AR 530–1
(Operations Security (OPSEC)).

AR 530–2
(Communications Security).

(C) AR 530–3
(Electronic Security) (U).

(S) AR 530–4
(Control of Compromising Emanations) (U).

AR 700–127
(Integrated Logistic Support (ILS)).

AR 700–129
(Integrated Logistic Support Management of Multiservice Communications-Electronics Systems and Equipment).

AR 1000–1
(Basic Policies for Systems Acquisition).

FM 5–20
(Camouflage).

FM 32–30
(Electronic Warfare, Tactics of Defense).

FM 90–2 (HTF)
(Tactical Deception (How to Fight Series)).

FM 101–5
(Staff Officers' Field Manual: Staff Organization and Procedure).

Section III
Prescribed Forms
This section contains no entries.

Section IV
Referenced Forms
This section contains no entries.

Glossary

Section I
Abbreviations
This section contains no entries.

Section II
Terms

Camouflage.
The use of concealment and disguise to minimize the possibility of detection or identification of troops, materiel, equipment, and installations. It includes taking advantage of the natural environment and the application of natural and artificial materials.

Command, Control, and communications countermeasures (C^3CM).
The integrated use of OPSEC, military deception, EW, and physical destruction supported by intelligence to deny information, degrade, or destroy enemy C^3 capabilities and at the same time protect friendly C^3 against such actions.

Concealment.
Measures taken to protect friendly forces and their materiel from enemy visual and photographic observation.

Countersurveillance.
Measures taken to prevent hostile surveillance of a force, area, or place. It includes counter-reconnaissance, electronic countermeasures, and other countermeasures to deny enemy use of sensors.

Electromagnetic camouflage.
The use of electromagnetic shielding, absorption, and enhancement techniques to minimize the possibility of detection and identification of troops, materiel, equipment, or installations by hostile sensors, using radiated electromagnetic energy.

Electromagnetic cover and deception.
The suppression, control, alteration, or simulation of electromagnetic radiation's associated with friendly systems, equipment, devices, or weapon components; they are used to deny an enemy a source of knowledge of the location of combat elements or mislead the enemy about their capabilities and intentions. These tactics include emission control (EMCON), signature suppression, profile alteration, and manipulative and simulative electronic deception aspects of ECM.

Electronic deception.
The deliberate radiation, radiation, alteration, absorption, or reflection of electromagnetic energy in a manner intended to mislead an enemy in the interpretation of use of information received by the enemy's electronic systems.

Imitative electronic deception (IED).
The introduction of radiation's into enemy systems that imitate the enemies' emissions.

Manipulative electronic deception (MED).
The alteration of friendly electromagnetic emission characteristics, patterns, or procedures to eliminate revealing, or convey misleading, tell-tale indicators which may be used by hostile forces.

Operations security (OPSEC).
The protection of military operations and activities resulting from the identification and subsequent elimination or control of intelligence indicators (vulnerabilities) which are susceptible to hostile exploitation.

Simulative electronic deception (SED).
The creation of friendly electromagnetic emissions to represent notional or actual capabilities to mislead hostile forces.

Tactical deception.
Actions at Corps level or below which mislead the enemy and induce him to do something counter to his interests. It includes manipulating, distorting, or falsifying evidence available to the enemy to insure security to real plans, operations, or activities.

Section III
Special Abbreviations and Terms

This section contains no entries.

USAPA

ELECTRONIC PUBLISHING SYSTEM
OneCol FORMATTER .WIN32 Version 1.10

PIN: 051257–000
DATE: 04-19-00
TIME: 14:54:49
PAGES SET: 13

DATA FILE: C:\WINCOMP\mark.fil
DOCUMENT: AR 525–21
DOC STATUS: NEW PUBLICATION