COUNTERINTELLIGENCE

CI // FIELD MANUAL
[RDCTD]

DETECT. ASSESS. INVESTIGATE. DECEIVE. NEUTRALIZE. LEARN.

A COVERT OPERATIVE'S PERSPECTIVE

THE MISSION

Counterintelligence (CI) is the continuous process of protecting people, operations, and information from foreign intelligence services, insiders, and other threats.
It is offensive, defensive, and deceptive by nature.

CI DOCTRINE

ANTICIPATE
Expect adversary intent and capability.

OBSERVE
See the indicators others overlook.

CONFIRM
Validate before you act.

CONTROL
Shape the environment and the narrative.

PROTECT
Deny, disrupt, and degrade threats.

OPERATOR TOOLS

HUMAN INTELLIGENCE (HUMINT)
Build sources. Read behaviors.

TECHNICAL SURVEILLANCE (TECHINT)
Collect signals. Map patterns.

OPEN-SOURCE INTELLIGENCE (OSINT)
Exploit what's publicly exposed.

COUNTER-SURVEILLANCE (CS)
Detect attempts. Break contact.

DECEPTION & MANIPULATION (DECM)
Control perception. Create distance.

OPERATIONAL SECURITY (OPSEC)
Deny information. Reduce risk.

SOURCES

Derived from:
- NISPOM (DoD 5240.02, 2024)
- NSA/CSS CI Fundamentals (2023)
- CIA CI Mission Center Guidelines (2024)
- Allied CI Best Practices (FVEY, 2024)
- Open-source reporting through May 2024

THE ENEMY ADAPTS. SO DO WE.

Stay sharp. Stay unseen.
Stay in the fight.

01 DETECT

Identify indicators of hostile intelligence activity through human, technical, and environmental observation.

- Monitor for anomalous behavior
- Track patterns and deviations
- Leverage multi-source collection
- Maintain persistent situational awareness

INDICATORS
- Unusual Interest
- Elicitation Attempts
- Surveillance Detection
- Data Probing
- Insider Risk Signals

THREAT PROBABILITY
45%

02 ASSESS

Determine the nature, intent, and capability of the threat. Prioritize based on risk to mission and assets.

- Evaluate threat actor profile
- Determine collection objectives
- Assess access and potential impact
- Assign threat level and response options

THREAT ASSESSMENT

ACTOR:	Foreign Intelligence Service
CAPABILITY:	High
INTENT:	Collect / Exploit
ACCESS:	Moderate
RISK TO MISSION:	High
RECOMMENDATION:	Investigate

THREAT LEVEL
LOW | MODERATE | **HIGH** | CRITICAL

03 INVESTIGATE

Conduct a focused CI investigation to confirm the threat, uncover methods, and identify assets and infrastructure.

- Develop investigative plan
- Collect corroborating evidence
- Identify networks and cutouts
- Document and establish attribution

EVIDENCE BOARD
- Meetings
- Communications
- Financial Links
- Travel Patterns
- Digital Footprint

CONFIDENCE LEVEL
82%

04 DECEIVE

Use deception to mislead the adversary, protect assets, and shape their decisions. Control the narrative.

- Create false signals and personas
- Manipulate collected information
- Redirect adversary collection
- Exploit their assumptions and biases

DECEPTION PLAN

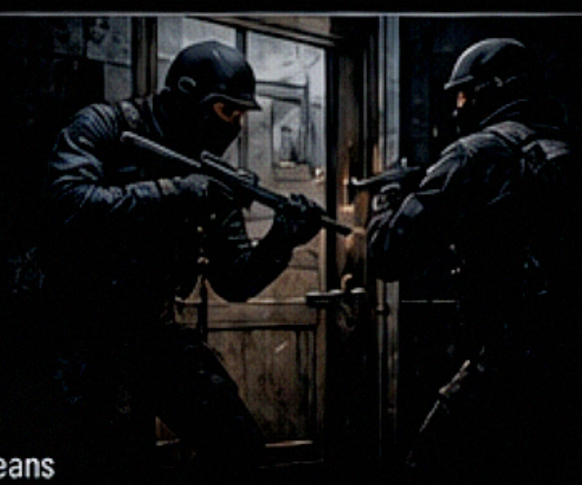
OBJECTIVE:	Mislead Collection
METHOD:	False Persona
CHANNEL:	Controlled Legend
TARGET:	Foreign Intel Officer
DESIRED EFFECT:	Wrong Target

DECEPTION STATUS
ACTIVE

05 NEUTRALIZE

Disrupt, degrade, or deny the adversary's ability to collect, operate, and achieve their objectives.

- Remove or isolate the threat
- Seize or secure compromised material
- Deny access to assets and information
- Apply legal, technical, and operational means



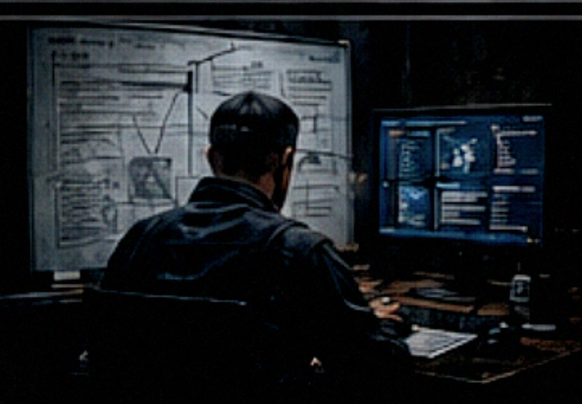
NEUTRALIZATION OPTIONS
- Disrupt Infrastructure
- Arrest / Detain
- Technical Denial
- Legal Action
- Exfiltrate Asset

MISSION IMPACT
THREAT NEUTRALIZED ✓

06 LEARN

Extract lessons, improve defenses, and strengthen the CI posture. Every operation makes the next one stronger.

- Conduct after-action review
- Update threat models and indicators
- Refine tactics, techniques, and procedures
- Train and disseminate lessons learned



LESSONS LEARNED
- Adversary used cutout network
- Targeted insider for access
- Improved insider vetting
- Increase monitoring of cutouts
- Enhance deception playbook

CI POSTURE
IMPROVED

COUNTERINTELLIGENCE IS A MINDSET. NEVER OFF DUTY. NEVER UNPREPARED.