INTRODUCTION TO
U.S. COUNTERINTELLIGENCE

“CI 101 -- A PRIMER”

1 July 2005

by

Mark L. Reagan, COL USA (Ret)

mmreagan@msn.com

The views and comments expressed in this paper are those of the author and do not necessarily reflect the official policy or position of the Department of Defense, the Office of National Counterintelligence Executive, or the United States Government.
“We must develop effective espionage and counterespionage services and must learn to subvert, sabotage and destroy our enemies by more clever more sophisticated and more effective methods than those used against us.”

-- Doolittle Report (1954)

“Counterintelligence means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities...”

-- Current U.S. Government Definition of Counterintelligence

1 Presidential directed “Special Study on U.S. Covert Activities” prepared by Lieutenant General James Doolittle in 1954.

2 Executive Order 12333, United States Intelligence Activities, 4 December 1981; counterintelligence is defined at section 3.4, subparagraph (a); copy of E.O. 12333 available on line at http://www.odci.gov/cia/information/fo12333.html.
Introduction to U.S. Counterintelligence  
“CI 101 – A Primer”

**Agenda**

- Introduction
- Historical Background
- Counterintelligence Defined
- Counterintelligence -- *an Intelligence Activity*
- Key Principles of Counterintelligence
- United States Counterintelligence Community
- National Counterintelligence Executive (NCIX)
- Federal Bureau of Investigation (FBI) Counterintelligence
- Central Intelligence Agency (CIA) Counterintelligence
- Defense Counterintelligence
- Closing Thoughts
- Appendix A – The Traditional Counterintelligence Functions
- Appendix B – Four Core Defense Counterintelligence Mission Areas

---

*The greatest enemy of successful counterintelligence is not a spy, but incorrect perceptions of counterintelligence* ³

---

**Introduction**

This paper provides a general introduction to U.S. counterintelligence -- a strategic national security instrument that is a unique intelligence activity... *both an operational capability and a strategic enabler*. Counterintelligence or CI is a complex discipline which is not easy to explain and even harder to fully comprehend... *much ambiguity, confusion and, at times, even disagreement exists*. The phrase *counterintelligence -- a wilderness of mirrors*⁴ best captures the essence of this ambiguity.

> "Outside of the CI community there is limited understanding of CI capabilities and limitations..."

-- IDA Study “Roles and Missions for DoD CI” (Oct 2003)

Many view counterintelligence as broken. Perhaps William Webster, former FBI Director and Director of Central Intelligence, described the CI dilemma best when he said –

> "...when you are not catching spies you are accused of having bad counterintelligence and when you are catching spies you are accused of having bad counterintelligence. You cannot have it both ways."

-- William Webster, Former DCI (1985)

Counterintelligence is much more than merely “catching spies” -- it is concerned with understanding and exploiting or neutralizing, all aspects of foreign intelligence activities directed against U.S. interests. The strategic importance of counterintelligence is often ignored and misunderstood by many, and under appreciated by most... *in fact few disciplines are so distorted or misrepresented by its critics.*

> "There are far too many in the Intelligence Community who either do not understand counterintelligence or, who understanding its concepts, have climbed to the top of their career ladders by opposing it."

-- Senator Malcolm Wallop, Senate Intelligence Committee (1985)

Counterintelligence is a fascinating and challenging discipline. Hopefully this paper will provide the reader with a basic understanding and appreciation of counterintelligence. This paper is not meant to be all inclusive but rather an overview of strategic U.S. counterintelligence... *CI 101 -- A Primer.*

---

Only unclassified, open source references/materials were used to compile this paper.

**Historical Background**

- As espionage is ancient, so is counterintelligence…
  
  "[I]t is essential to seek out enemy agents who have come to conduct espionage against you..."  
  -- Sun Tzu, *Art of War*, circa 500 B.C.

- Since the founding of the Republic, counterintelligence has historically played a key role in U.S. national security, especially in its unique ability in supporting efforts to shape and influence adversary decision makers – military, intelligence, and political… *CI an integral part of American history*

- During the Revolutionary War, George Washington was an avid user of intelligence and counterintelligence as well as a consummate practitioner of the intelligence craft… not only did he understand and appreciate the value of counterintelligence, he also made excellent use of offensive counterintelligence operations

- Counterintelligence played a critical role in World War II, DESERT STORM (Persian Gulf War of 1991), and Operation Iraqi Freedom (OIF) to name a few… *demonstrating its value as a force multiplier and operational capability*

- Recommended Reading: For a comprehensive historical background on counterintelligence see the multi-volume *Counterintelligence Reader* published by the Office of the National Counterintelligence Executive.5

---

Counterintelligence Defined

- There are many definitions and numerous descriptions of counterintelligence

- 1958 Government definition of counterintelligence --

  **Intelligence activity… protecting the security of the nation**

  “...intelligence activity, with its resultant product, devoted to destroying the effectiveness of inimical foreign intelligence activities and undertaken to protect the security of the nation and its personnel, information, and installations against espionage, sabotage, and subversion.

  ...includes the process of procuring, developing, recording, and disseminating information concerning hostile clandestine activity and of penetrating, manipulating, or repressing individuals, groups, or organizations conducting such activity.” 6

  -- National Security Council Intelligence Directive 5

- 1969 CIA special study outlined the function and goal of a counterintelligence service --

  “Generally speaking, the function of the internal counterintelligence service is to protect the lawfully constituted government against concealed attack.

  ...the CI service is properly concerned only with hostile clandestine and covert activity. Clandestine activity is that which the enemy tries to conceal totally. It usually takes the form of espionage, counterespionage, subversion, or—much more rarely—sabotage. Covert activity is not fully concealed; in fact, it is likely to take the form of a newspaper article or radio broadcast, or even terrorism, for which the widest possible publicity is sought. What the enemy tries to hide in this type of action is his sponsorship or other involvement.

  The goal of the CI service is to learn everything it can about these two kinds of inimical action, and therefore about people carrying out the action, without letting these persons become aware that the service is acquiring such information.

  Only by making available to the government information about its enemies which is complete enough to include all essentials and which was acquired secretly, so that the enemies remain unwarned, can the counterintelligence service do the task for which it was created and designed.” 7

  -- CIA Special Study (1969)

---


• In 1976, The Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (aka Church Committee), chaired by Senator Frank Church, described counterintelligence --

**Counterintelligence**

*Introduction...*

**Counterintelligence is intelligence activity dedicated to undermining the effectiveness of hostile intelligence activities**

- A “special form” of intelligence activity, separate and distinct from other disciplines
- Its purpose is to discover hostile foreign intelligence operations and destroy their effectiveness
- Involves the protection of the US Government against infiltration by foreign agents, as well as the control & manipulation of adversary intelligence operations
- An effort is made to both discern and deceive [sic] the plans & intentions of enemy intelligence [efforts]

Counterintelligence wages nothing less than a secret war against antagonistic intelligence services

The Church Committee referred to counterintelligence as “…the most secret of secret intelligence activities—the heart of the onion.”

In 1985, Francis McNamara (The Nathan Hale Institute), described counterintelligence as “…intelligence of a special kind, plus something else.”

Counterintelligence according to FBI Assistant Director Dave Szady --

“It's much broader than just espionage--the traditional spy game. It also includes the protection of our critical national assets. And by that, I don't mean the bridges, the railroad stations, the nuclear plants. I mean things like our country's advanced technologies, its weapons systems, its military capacities--classified information and systems that are strategically important to our nation's well-being. [CI] also involves protecting trade secrets and guarding against operations or disinformation campaigns that would disadvantage the U.S.”  

CI is used to defeat and exploit foreign intelligence services and others (e.g., terrorists, foreign criminal enterprises, cyber intruders, etc.) who use clandestine/covert activities and operations to harm and disadvantage U.S. interests... CI is a national security tool

---

• The United States Intelligence Community (IC) website provides that -- 

*The IC is faced with “…the problem of identifying, understanding, prioritizing and counteracting the intelligence threats (from foreign powers) that are faced by the United States. This activity is known as counterintelligence.”*  

-- Intelligence Community Website

• Current Government definition of *counterintelligence* per Executive Order -- 

...information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities.  

-- Executive Order 12333

• Counterintelligence often viewed as “protecting secrets, frustrating attempts by foreign intelligence collectors to acquire those secrets, and catching [traitors] who spy for those foreign intelligence services.”  

11

• CI is much broader than just “protection focused”… *CI protects & exploits*

• Counterintelligence “embraces all activities, human and technical, whether at home or abroad, that are undertaken to identify, assess, neutralize and exploit foreign intelligence threats... counterintelligence is inherently a strategic, national security instrument.”  

-- Hon Michelle Van Cleave, NCIX (18 Nov 2004)

______

Counterintelligence wages “nothing less than a secret war against antagonist intelligence services”  

12

________________


10 Executive Order 12333, *United States Intelligence Activities*, 4 December 1981; this E.O. specifically notes that counterintelligence does not include “personnel, physical, document, or communications security programs.”


12 U.S. Senate Report 94-755, 26 April 76.
Counterintelligence is an intelligence activity. Although some continue to debate this premise, within the United States, by statute and policy, counterintelligence is an “intelligence activity” and is identified as such in the National Security Act, Executive Order, and various directives.

**National Security Act of 1947 (P.L. 80-253) -- as amended**

- Basic law governing intelligence in the United States, which specifically defines *intelligence* as including foreign intelligence and *counterintelligence*.

**Executive Order 12333 -- U.S. Intelligence Activities (4 Dec 1981)**

- Provides the U.S. Government definition for *counterintelligence*: “information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including personnel, physical, document, or communications security programs.” [para 3.4]

- Under goals (Part I) with respect to the national intelligence effort, it directs that “special emphasis should be given to detecting and countering espionage and other threats and activities directed by foreign intelligence services against the United States Government, or United States corporations, establishments, or persons.” [para 1.1(c)] …*this activity is part of counterintelligence*

- Directs the Intelligence Community to conduct *intelligence activities* necessary for “the protection of the national security of the United States, including… collection of information concerning, and the conduct of activities to protect against, intelligence activities directed against the United States, international terrorist and international narcotics activities, and other hostile activities directed against the United States by foreign powers, organizations, persons, and their agents.” [para 1.4(c)]

**Department of Defense Directive 5240.1 -- Intelligence Activities (25 Apr 1988)**

- Intelligence activities defined as “the collection, production, and dissemination of foreign intelligence and *counterintelligence* by the DoD intelligence components…” [para 3.1]

- “DoD Intelligence Components include… US Army Intelligence and Security Command (USAINSCOM); counterintelligence elements of the Naval Criminal Investigative Service (NCIS); counterintelligence elements of the Air Force Office of Special Investigations (AFOSI); and the 650th Military Intelligence Group…” [para 3.4]"

---

*Counterintelligence is intelligence activity focused on undermining the effectiveness of -- as well as exploiting -- adversary intelligence activities*
**Key Principles of Counterintelligence**

- CI acknowledged in Senate Report 94-755 as a “special form” of intelligence activity… separate and distinct from the traditional intelligence disciplines (INTs)

- Counterintelligence is a unique intelligence discipline… as is foreign intelligence (FI)

- Foreign intelligence focuses on collecting information to learn adversaries’ secrets, whereas CI focuses on countering & exploiting foreign intelligence activities
  - Espionage… stealing others’ secrets
  - Counterintelligence… preventing others from stealing our secrets, as well as exploiting their collection efforts directed at us

- Foreign Intelligence & Counterintelligence… equally important strategic assets, which focus on distinctly different content, as well as outcomes

**Counterintelligence**

**Foreign Intelligence vs. CI…**

*It is the job of [foreign] intelligence to collect and analyze information. Espionage for this purpose… acts only with the objective of getting past the opposing counterintelligence and security forces as uneventfully as possible.  

...Counterintelligence, on the other hand, is engaged in covert war, all-out and immediate. It has to take action—at home by investigating, arresting, interrogating, doubling, and prosecuting [foreign intelligence] operatives, and abroad by carrying out recruitment, neutralization, harassment, diversionary, and psywar operations against their secret service system.*


- Per Executive Order 12333, counterintelligence is “information” and “activities conducted” …hence CI is both knowledge and action --
  - Knowledge of foreign intelligence activities directed against U.S. interests
  - Action to frustrate and exploit those activities

- CI is a collector as well as a consumer of intelligence… although not considered a traditional INT, it can provide valuable intelligence

- CI can supply unique insights into the actions of our adversaries and the clandestine/covert threats directed against us, as well as provide opportunities for advancing our own interests

- CI counters espionage directed at us by a wide variety of adversaries and sometimes even friends… espionage long proven the highest leveraged means of defeating U.S. capabilities
• CI is critical in wartime to defeat & exploit adversary intelligence capabilities

• CI “bridges” foreign intelligence, law enforcement, security/homeland security, and combating terrorism (CbT)… all mutually supportive but each distinctly different

Counterintelligence
A “bridging” discipline…

Mutually supportive… yet each distinctly different

What Counterintelligence is NOT…

• CI is not HUMINT… often confused with human intelligence

CI versus HUMINT

<table>
<thead>
<tr>
<th>COUNTERINTELLIGENCE</th>
<th>HUMAN INTELLIGENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mission: deter, detect &amp; neutralize Foreign Intel Activities/Espionage</td>
<td>Mission: overtly and/or clandestinely acquire intel info via human sources</td>
</tr>
<tr>
<td>Focus: adversary collectors</td>
<td>Focus: obtaining foreign secrets</td>
</tr>
<tr>
<td>Seeks out foreign intelligence collectors… engages the threat</td>
<td>Seeks to avoid foreign CI… uses CI to protect its own operations</td>
</tr>
<tr>
<td>Impacts adversary’s knowledge of US</td>
<td>Shapes our understanding of adversary</td>
</tr>
<tr>
<td>Collection one of five CI functions*</td>
<td>Collection is the Mission</td>
</tr>
<tr>
<td>CI Requirements &amp; Threat Driven</td>
<td>Requirements Driven</td>
</tr>
<tr>
<td>Key Players: FBI, CIA, Military Services, and DoD Agencies</td>
<td>Key Players: CIA-Directorate of Operations (DO) &amp; DIA-Defense HUMINT</td>
</tr>
</tbody>
</table>

* Neutralization is the primary mission… collection is secondary

Although CI & HUMINT are different disciplines… they have interdependencies & can be mutually supportive

Note: Clandestine military HUMINT operations discussed at [http://www.fas.org/irp/offdocs/int014.html](http://www.fas.org/irp/offdocs/int014.html)
• CI is not Security... CI transcends the purely defensive nature of security.\(^{13}\)

```
“CI attacks the actor. It attacks the opposition intelligence structure. It is not speculative. CI feeds security because it helps them focus on meaningful measures and safeguards. Using CI to help security is just smart security.
```

-- Robert P. Hanssen (Soviet Spy, former FBI Agent & current federal inmate)\(^{14}\)

• CI vs. Security… security only protects it does not “attack”

### Counterintelligence versus Security

<table>
<thead>
<tr>
<th><strong>Activities</strong></th>
<th><strong>Counterintelligence</strong></th>
<th><strong>Security</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>CI Investigations</td>
<td>• CI Operations (Defensive &amp; Offensive)</td>
<td>• Physical Security/Facilities Protection</td>
</tr>
<tr>
<td>• CI Collection/Liaison</td>
<td>• CI Collection/Liaison</td>
<td>• Industrial &amp; Personnel Security</td>
</tr>
<tr>
<td>• CI Analysis/Production</td>
<td>• CI Analysis/Production</td>
<td>• Personnel Security Investigations</td>
</tr>
<tr>
<td>• CI Services to include TSCM, CI polygraphs, CI training &amp; awareness, etc.</td>
<td>• CI Services to include TSCM, CI polygraphs, CI training &amp; awareness, etc.</td>
<td>• AIS/Information Systems Security</td>
</tr>
</tbody>
</table>

| Focus: | Sword directed at the adversary collector... identify/understand/counter adversary collection efforts ...mission driven | Shield to protect friendly activities... establish/adhere to standards; fix system weaknesses ...rule driven |
| Objective: | deter/detect/disrupt/control adversary collection ...reduce or control "threat" | deny/prevent unauthorized access ...reduce "vulnerability" |
| Perspective: | adversary’s perspective ...looking "outside - in" | internal perspective ...looking "inside - out" |
| Concern: | clandestine & covert threats | unauthorized access |
| Key Authorities: | EO 12333; NSPD-1; PDD-24; PDD-75; PDD-83; CI Enhancement Act of 2002; DoDD 5240.2; and DoDI 5240.1 | EO 12958, 12968 & 12829; PDD-63; NSSD-298; DoDD 5200.1/8/28; DoD 5200.1-R/2-R; 5200.8-R; & 5220.22-R/M |
| Nat’l Board: | National CI Policy Board (NCIPB) | PCC/RA & IS (Records Access & Info Security) Security Policy Board (SPB) originally established Sep 94 (PDD-29) was abolished via NSPD-1 (13 Feb 2001) |

*Mutually Supporting... protecting critical resources & secrets*

• Security focuses on protecting friendly sensitive information and secrets from unauthorized access… it does not directly engage foreign intelligence threats

• Risk Management… where CI and Security intersect\(^{15}\)
  - Close partnership required to ensure security directives are based on the “threat”
  - Prior strategy of risk avoidance too resource intense and not cost effective
  - Threat assessments are critical for security & security countermeasures policymakers
  - Counterintelligence provides the “window” into the adversary threat
  - Today’s security protection must be “rational, threat-appropriate and cost effective”

\(^{13}\) Security is defined as: 1) Measures taken by an activity to protect itself against all acts designed to, or which may, impair its effectiveness; 2) A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences; or 3) With respect to classified matter, the condition that prevents unauthorized persons from having access to official information that is safeguarded in the interests of national security. (Joint Pub 1-02)

\(^{14}\) Robert P. Hanssen as quoted in “Diary of a Spy” by Paul M. Rodriquez, Insight on the News, 16 July 2001

\(^{15}\) Risk management is the process of identifying, assessing, and controlling, risks arising from operational factors and making decisions that balance risk cost with mission benefits (DoD Dictionary – Joint Pub 1-02); a security philosophy which considers actual threats, inherent vulnerabilities, and the availability and costs of countermeasures as the underlying basis for making security decisions (Joint Security Commission Report, 1994).
Counterintelligence – essential for sound risk management

“Getting ...the threat information necessary to support coherent, risk-based security countermeasures...is an ad hoc rather than a systematic process. In the absence of access to threat assessment information, security policies have been based on risk avoidance, constrained primarily by the availability of resources.”


- Effective CI and security are integral to program efficiency, combat, and operational effectiveness, and foreign policy success… mutually supportive but yet distinct

“Security and counterintelligence serve as the foundation of the Intelligence Community. As with any sound foundation, its parts are mutually supportive.”

-- George Tenet, Director Central Intelligence, in “The DCI's Strategic Plan for Personnel Security...”

- Counterintelligence is not synonymous with Law Enforcement (LE)... although there are similarities and they can be mutually supportive

Law Enforcement versus Counterintelligence

LE is police work waging a war against crime… evidence–prosecution centric
CI is national security work waging a war against foreign clandestine & covert threats… information–exploitation centric

- CI vs. LE --
  - Operate in fundamentally dissimilar manners… different legal authorities, different oversight structures, and different governing paradigms
  - Counterintelligence… primarily focused on identifying, collecting on, and exploiting foreign intelligence activities/clandestine & covert threats – proactive action
  - Law Enforcement… focused on investigating, arresting, and prosecuting those who violate criminal laws – reactive response (uses ex post facto arrests and trials governed by rules of evidence)
  - These two specialties merge or intersect when hidden intelligence activity is also criminal… national security crimes (e.g., espionage, treason, spying, sedition, etc.)
  - Primary difference… in targets and timing rather than methods

- Criminal investigations & counterintelligence investigations… many basic investigative skills and methods applicable to both [following list is not all inclusive] --
  - Legal principles, to include rules of evidence, rights warning, etc.
  - Records checks, elicitation, interviews, interrogations, courtroom testimony, etc.
  - Search and seizure, including collecting, processing and preserving evidence
  - Investigative reporting writing, sworn statements, waiver of rights, etc.
  - Specialized investigative techniques, e.g., confidential sources, undercover operations, physical surveillance, electronic surveillance, concealed monitoring, etc.
  - Penetration of clandestine/secretive closed organizations
- **CI vs. LE… different cultures**

  [LE] wants to identify bad guys and put them in jail. [Intel/CI] wants to identify bad guys and follow them or recruit them, so they can keep getting information from them. These are different cultures…

  -- Robert M. Gates (2 Feb 1996)  
  Former DCI

- **CI vs. LE… a Defense view**  

  **Counterintelligence**

  **CI vs. Law Enforcement... DoD Report**

  - Services have different approaches to CI due to their unique missions
  - Navy & Air Force doctrine: CI primarily a law enforcement mission
  - Army doctrine: CI, first & foremost, an intelligence mission
  - Lines of jurisdiction between many traditional law enforcement activities, criminal intelligence activities, CI activities, and positive intelligence collection activities are, and should be, by nature blurred
  - Attempting to demarcate the disciplines… artificially is difficult and not in the best interest of DoD
  - Counterintelligence is not strictly a law enforcement matter… nevertheless CI is not strictly intelligence

  *Separate but parallel interests…*

  Prepared by Mark L Reagan – 8 May 2003


- A Special DoD Advisory Board found that “**considerable intersection exists** between law enforcement, counterintelligence, and intelligence...” and it specifically noted that --

  “…the intelligence and law enforcement communities need to improve their understanding of their respective needs and operating practices and cooperate earlier, more closely, and more consistently on matters in which they have separate but parallel interests”  

- Within DoD, law enforcement activities by the Air Force Office of Special Investigations and the Naval Criminal Investigative Service have facilitated the collection of relevant threat information from a variety of foreign sources

---

16 As quoted in “Overview: After the Aldrich Ames Spy Scandal,” by Mary H. Cooper, CQ Researcher, Vol 6, No 5, 2 Feb 1996


18 Ibid, pg. 70.
• Counterintelligence can be viewed as a “bridge” between law enforcement and foreign intelligence… *information obtained by any of one of these disciplines may potentially be of value and use to the others*

(CI a bridging discipline which also bridges to *security* and *combating terrorism* as discussed earlier)

• Law enforcement is often in the best position to detect indicators of terrorist planning and execution.

• LE and CI are distinct disciplines… *yet they are mutually supportive and complement one another as collaborative partners in protecting U.S. national security interests* ¹⁹

---

**Counterintelligence a unique “bridging discipline”**

• CI is a critical function deemed essential by most nation states to the effective pursuit of both their national interest and national security… *it is an instrument of national policy*

**US Government CI**

*CI an instrument of national policy*

To protect sensitive national security information, it is critical for us to effectively counter the collection efforts of foreign intelligence services and non-state actors through vigorous counterintelligence efforts…

-- National Security Strategy (NSS)*

*...it is critical that the U.S. maintain a highly effective and coordinated counterintelligence capability*

**Espionage is an instrument of national policy… CI is the instrument of national policy which counters foreign intelligence activities**

Prepared by Mark L. Reagan – 9 May 2003

• Counterintelligence represents a philosophic approach that can bring coherence to many areas of national policy --

  o Counterintelligence enables successful execution of sensitive national security operations… *to include foreign intelligence activities and operations*
  o CI must be an integral part of the entire intelligence process… *intelligence is vital to the formulation and execution of U.S. policy and to the nation’s security*
  o Significant failures in CI can produce damaging failures in intelligence, in both collection and analysis, and negate enormous investments in sensitive intelligence capabilities… *we must safeguard the integrity of intelligence – both FI & CI*

**CI plays a critical role in ensuring the reliability of U.S. intelligence**

"Intelligence requires secrets…. The future of US intelligence effectiveness depends to a very significant degree on keeping its secrets about collection sources and methods and analytical techniques. When secrecy is breached, foreign targets of US intelligence—such as adversary countries and terrorists—learn about, and then often develop countermeasures to, US intelligence techniques and operations. As a result, the effectiveness of intelligence declines, to the detriment of the national security policymakers and warfighters, and the citizenry that it is meant to serve."


• CI is a unique & valuable operational capability… *it can proactively influence decision and knowledge management outcomes of specific adversaries and competitors*
• CI capabilities are high-demand low-density resources… *CI efforts must be focused*

• **National Core CI Issues** as identified in PDD-75 20 --
  - Detection and neutralization of espionage
  - CI support to protection of U.S. persons, critical information, and assets
  - CI support to the protection of research & development (R&D) and technology
  - CI support to the protection of critical infrastructure including economic security
  - CI support to the protection against covert foreign influence and manipulation

• On 1 March 2005, the President approved a new *National Counterintelligence Strategy* 21 which identified the following **Strategic CI Objectives** --
  - Identify, assess, neutralize and exploit foreign powers, terrorist groups, international criminal organizations, and other entities who seek to do us harm
  - Protect our intelligence collection and analytical capabilities from adversary denial, penetration, influence, or manipulation
  - Enable the successful execution of our sensitive national security operations
  - Safeguard our vital national security secrets, critical assets, and technologies against theft, covert foreign diversion, or exploitation

• CI enhances National Security… *an operational capability & strategic enabler*

• Full-spectrum counterintelligence… *encompasses a wide range of activities from defensive (reactive) to offensive (proactive)*

• Robust aggressive CI is critical… *the first commandment of CI is be offensive*

  *Our CI mindset should be relentlessly offensive. We need to go after our CI adversaries.* 22

  -- James M. Olson, Former Director, CIA Counterintelligence Center

• The “new” direction for U.S. counterintelligence… *is global proactive engagement*

  *U.S. counterintelligence will shift from a reactive posture to a proactive strategy of seizing advantage.* 23

  -- The National Counterintelligence Strategy

---


• U.S. Counterintelligence to go on the offensive --

**Offensive counterintelligence**, put into a larger context, can be used --

-- to diffuse or shape an emerging threat,
-- to influence key decisions of our adversaries,
-- to mask vulnerabilities, to advance diplomatic objectives, or
-- to confer advantages on the negotiating table or on the battlefield...

_In wartime, we must be able to defeat the adversary’s intelligence capabilities, including their ability to deceive or mislead us..._

_Strategic CI planning can also increase the options available to decision-makers for advancing national objectives while avoiding war._

-- Hon Michelle Van Cleave, National Counterintelligence Executive as quoted in “Inside the Navy,” 23 Nov 2004

• Essential to the success of counterintelligence --

_Aggressive double agent (DA) operations...[and] penetration. For every American spy, there are several members of the opposition service who know who he is or she is. No matter what it takes, we have to have penetrations._

-- James M. Olson, Former Director, CIA Counterintelligence Center

• The traditional functions of counterintelligence -- see Appendix A for details

---

Full array of active and passive (offensive & defensive) measures to protect friendly activities from adversary exploitation and manipulation

• Globally engaged... every day counterintelligence executes its wartime mission --

“...[Counterintelligence] is performing its wartime mission every day as agents counter foreign intelligence threats – that’s why we call it the Silent War.”

-- COL Stuart Herrington, USA (Ret)
• The President’s charge for Counterintelligence today --

“…identify and access what foreign intelligence services are doing against U.S. interests and how they are doing it, and develop doctrine, assign resources and implement operations to neutralize those activities proactively at home and abroad.”  

• Seven Pillars of US CI Strategy  as identified by the National CI Executive --

\[
\begin{align*}
\text{US Government CI} \\
\text{Seven Pillars U.S. CI Strategy...}
\end{align*}
\]

- Extend the safeguards of strategic CI to the Global War on Terrorism
- Shift emphasis from a posture of reacting to a proactive strategy of seizing advantage
- Protect the vital technology secrets that are the bedrock of our strategic security
- Safeguard the integrity of intelligence and identify & defeat foreign denial, deception and covert influence operations
- Help level the economic playing field so that U.S. business and industry are not disadvantaged by unfair intelligence practices of foreign competitors
- National security decision-making process must be informed by CI insights
- National CI system to enable the execution of the National CI Strategy

• Counterintelligence “is and ought to be at the forefront of the general movement of intelligence [and at] the center of U.S. projection of national power and influence.”  

-- Roy L. Reed & Anthony D. Mc Ivor

\[\text{Counterintelligence -- an instrument of national security}\]

\[\begin{align*}
24\text{“The National Counterintelligence Strategy of the United States,” speech by Hon Michelle Van Cleave on 5 March 2005, pg. 9; copy available on line at } \text{http://www.ncix.gov/publications/reports_speeches/speeches/CI21Conf/TexasspeechCI.pdf.}
\end{align*}\]

\[\begin{align*}
25\text{Ibid, pp. 3-8.}
\end{align*}\]

\[\begin{align*}
26\text{Roy L. Reed and Anthony D. Mc Ivor, “Making the Case: Counterintelligence as a Strategic Asset,” American Intelligence Journal (Spring/Summer 2004), pg. 46.}
\end{align*}\]
United States Counterintelligence Community

• Macro View… The Key Players

US Government CI
Macro View -- The Key Players...

US Counterintelligence is a conglomerate of services, agencies, and components with varying responsibilities, jurisdictions, and capabilities...

› National CI Executive (NCIX)… authorized by PDD 75 (replaced NACIC)
› FBI… policy & coordination at CI Div at HQ – Field Offices execute
› CIA… Counterintelligence Center (CIC) at Headquarters
› DoE… Office of CI (OCI) at HQ [all CI Policy w/in DoE] & Office of Defense Nuclear CI (DNCI) at the Nat’l Nuclear Security Admin (NNSA)
› DoS… CI within Diplomatic Security at HQ (Office of Investigations & CI)

Primary US CI

Largest U.S. Government Agency/Department

• huge global footprint

Macro View… The CI Community

Counterintelligence Community
U.S. Government...

White House

Congressional Oversight

Statutory Head of US CI

National CI Executive (NCIX)...

National CI Policy Board

• Nat’l Exec., Chief
• Nat’l Chiefs, Vice Chairs
• Senior Staff
• Nat’l CI Policy Subcom., CIC, OCI

Office of NCIX

• Nat’l Threat Identification & Prioritization Assessment
• Nat’l CI Strategy Analysis
• Nat’l CI Counter & Targeting Coordination
• Nat’l CI Outreach, Warning, and Warning

USCG

DHS

DoJ

DoD

DoE

DOD

NNSA

• Regional x 6
• Functional x 11

Statutory Advisors

CJCS & DNI

NSC/PC

NSC/DC

NSC/IPC

Naturalized cafes

USG

FBI

CIA

CMS

DOD

USD-I

DO

DS/DO/ICI

New Dir of Nat’l Intelligence


Dir NCTC reports to DNI per EO 13354 (27 Aug 04)

PL 108-458 (17 Dec 04)

on planning & progress of joint CT ops Dir NCTC reports direct to POTUS per PL 108-458 (17 Dec 2004)

DNCI

OIC

CISO

CJ2

NCS

NSC

HPSCI

SSCI

White House

House

Senate

Proponent

Vice Press

Sec State

Sec Defense

Pres

Vice Pres

Statutory

National CI

Policy Board

Chair

Senior Reps from--

DoJ (incl FBI)

DoD (incl Joint Staff)

DoS

DoE

CIA

Others as specified by the President

Section 902*

Section 904 *

National CI Policy Board

• Nat’l Exec., Chief

Office of NCIX

• Nat’l Threat Identification & Prioritization Assessment

National CI Policy Board

• Nat’l Exec., Chief

Office of NCIX

• Nat’l Threat Identification & Prioritization Assessment

– the most CI resources, as well as --

– the most places…over 600 fixed facilities worldwide

– the most cleared people…over 2.4 million with clearances

– the most SECRETS…over 80% of all w/in US Government

Largest U.S. Government Agency/Department

• huge global footprint

Macro View… The CI Community
**National CI Executive (NCIX) --**

- Charge with leading and integrating the CI activities of the United States
- Established 1 May 2001 by PDD-75 as the *substantive leader of national-level CI*
- Appointed by the President and under the intelligence reform act reports to the new Director for National Intelligence (DNI)²⁷
- Advisory budget authority with little visibility into individual agencies’ CI operations; no current ability to assign operational responsibility or evaluate performance²⁸
- NCIX heads the Office of the National Counterintelligence Executive (ONCIX) and chairs the National Counterintelligence Policy Board (NCIPB)

**Office of the National CI Executive**

*Organization...*

- **Executive Officer**
- **NCIX Deputy**
- **Chief of Staff**
- **General Counsel**
- **Special Assistant**
- **Collections & Analysis**
- **Assessments**
- **Operations Support & Special Programs**
- **Strategy & Policy**
- **Collections & Analysis**
- **Analysis**
- **Community Programs & Resources**
- **Public Affairs, Training & Education**
- **Chief of Staff**
- **Security**
- **IT**
- **HR**
- **Logistics**
- **Budget/Contracts**
- **Assessments**
- **Assessments**
- **Legislative Affairs**
- **Executive Secretariat**
- **Executive Secretariat**

*Staffed by senior CI & other specialists drawn from across the national security community*

- ONCIX is an outgrowth from CI-21 and PDD-75; it replaced the National Counterintelligence Center (NACIC)²⁹
- In 2002 the NCIX was codified into law and its “center” renamed an “office”³⁰
- Recent WMD report identified the need for an *empowered NCIX* and recommended NCIX become the DNI’s *Mission Manager for Counterintelligence*³¹
- For additional information about the ONCIX go to [http://www.ncix.gov/](http://www.ncix.gov/)

---


²⁹ NACIC was addressed in PRD 44 and established under PDD-24 (May 1994) to coordinate and improve the effectiveness of CI activities across the U.S. Government


³¹ WMD Report, pp. 490-492.
- **Federal Bureau of Investigation (FBI)** --
  - Investigative arm of the Department of Justice with jurisdiction over violations of more than 200 categories of federal law; also a statutory member of the IC
  - Lead agency for counterintelligence within the United States
  - Centralized management and oversight of CI at the Counterintelligence Division

- **Central Intelligence Agency (CIA)** --
  - Primary responsibility for U.S. clandestine activities abroad including the conduct of clandestine counterintelligence outside the United States
  - Primary CI focus is mostly defensive, aimed primarily to protect CIA operations
  - Counterintelligence Center (CIC) at Headquarters

- **Department of Defense (DoD)** --
  - DoD, with its component CI units located within the military services, principally focuses on protecting the armed forces -- *broad overview of Defense CI follows*

---

32 NSCID 5, “U.S. Espionage and Counterintelligence Activities Abroad,” 17 February 1972 [para 3].

33 WMD Report, pp. 489-490.

34 CIA/CIC established in 1988 by DCI William Webster to mobilize and coordinate counterintelligence capabilities inside the CIA, and to integrate CIA’s counterintelligence work with the FBI and the Department of Defense.

35 WMD Report, pg. 490.

36 Ibid, pg. 492.
**Defense Counterintelligence**

- The business of the Department of Defense is national security… *national security cannot succeed without a viable CI program and robust CI capabilities*

- Department of Defense (DoD) Policy --

  *Counterintelligence activities shall be undertaken to detect, identify, assess, exploit, and counter or neutralize the intelligence collection efforts, other intelligence activities, sabotage, terrorist activities, and assassination efforts of foreign powers, organizations, or persons directed at the Department of Defense, its personnel, information, material, facilities and activities.*

  -- DoD Directive 5240.2  
  *DoD Counterintelligence* (22 May 1997)

- DoD Counterintelligence Vision --

  **DoD Counterintelligence Vision**

  *The integrated application of aggressive counterintelligence activities by highly capable professionals empowered by leading edge technologies to detect, deter, and defeat foreign intelligence activities, sabotage, terrorism and other clandestine or covert activities directed against DoD*  

  -- DoD Counterintelligence Strategy (16 Dec 2004)

- The focus of Defense CI is worldwide due to DoD’s national security mission and global footprint 37 --

  o Operates in more than 146 countries… *permanent bases & temporary deployments*
  
  o Over 3 million personnel… *over ½ million overseas or afloat*
  
  o Operates from more than 6,000 locations… *uses in excess of 30 million acres and 600,000 buildings & structures*

---

The Defense CI Challenge --

**DoD Counterintelligence**

*The Challenge...*

“Ensuring that DoD assets are defended from attack by foreign and hostile intelligence services...”

--- Dr. Stephen A. Cambone
Under Secretary of Defense for Intelligence (USD/I)

Source: Answers to advance congressional questions - 27 Feb 2003
(at that time Dr Cambone was the nominee for USD/I)

According to the National Defense Strategy (March 2005), “Uncertainty is the defining characteristic of today’s strategic environment...[with] an array of traditional, irregular, catastrophic, and disruptive capabilities and methods threaten[ing] U.S. interests.” -- Defense CI must be capable of operating seamlessly throughout today’s security environment, as well as responding to the emergence of developing threats

---

**Today's Security Environment**

*Persistent & Emerging Challenges...*

<table>
<thead>
<tr>
<th>IRREGULAR</th>
<th>CATASTROPHIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Those seeking to erode U.S. influence and power by employing unconventional methods, such as:</td>
<td>Those seeking to paralyze U.S. leadership and power by employing WMD or WMD-like effects in surprise attacks on symbolic, critical or other high-value targets, such as:</td>
</tr>
<tr>
<td>Terrorism</td>
<td>9-11 (11 September 2001)</td>
</tr>
<tr>
<td>Insurgency</td>
<td>Terrorist use of WMD</td>
</tr>
<tr>
<td>Civil War</td>
<td>Rogue missile attack</td>
</tr>
<tr>
<td>Emerging concepts, i.e., unrestricted warfare</td>
<td>Likelihood: moderate &amp; increasing</td>
</tr>
<tr>
<td>Vulnerability: moderate, if not effectively checked</td>
<td>Vulnerability: unacceptable; single event could alter American way of life</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TRADITIONAL</th>
<th>DISRUPTIVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Those seeking to challenge U.S. power by military operations, such as:</td>
<td>Those seeking to usurp U.S. power and influence by acquiring breakthrough capabilities, such as:</td>
</tr>
<tr>
<td>Conventional air, sea, and land attacks</td>
<td>Sensor operations</td>
</tr>
<tr>
<td>Nuclear forces of established nuclear powers</td>
<td>Biotechnology</td>
</tr>
<tr>
<td>Likelihood: decreasing (absent pre-emption) due to historic capability-overmatch and expanding qualitative lead</td>
<td>Miniaturization on the molecular level</td>
</tr>
<tr>
<td>Vulnerability: low, if transformation is balanced</td>
<td>Directed-energy and other emerging fields</td>
</tr>
<tr>
<td>Source: National Defense Strategy (March 2005)</td>
<td></td>
</tr>
</tbody>
</table>

The National Defense Strategy emphasizes “the importance of influencing events before challenges become more dangerous and less manageable” -- CI provides a critical operational capability in influencing desired strategic outcomes
• The key players in defense counterintelligence --

DoD Counterintelligence
The Players...

- OSD (USD/I) provides policy, planning guidance, and oversight
- Counterintelligence Field Activity (CIFA)… established 2002
  - CI Program Management, analytical services & CI integration
  - DoD focal point for National Counterintelligence Executive (NCIX)
  - Consolidates many DoD-level CI activities under one umbrella…
    e.g., JCAG, JCIITA, DoDPI, FPRG, DCIIS Program Office, etc.
- Military Departments
  - Army (INSCOM & 650th MI)… intelligence approach -- reports to Army G2
  - Air Force (OSI)… law enforcement approach -- reports to USAF IG
  - Navy (NCIS)… law enforcement approach -- reports to SECNAV
  - USMC (Tactical CI)… intelligence approach -- reports to Dir of Intelligence
- Defense Agencies/DoD Components with internal CI resources
  - NGA, NSA, NRO, DIA, Joint Staff (J2-CI), DTRA, DSS, and MDA
- Combatant Commands… CISOs are the CI focal point

DoD Counterintelligence – Global Footprint

• Current structure and organization of defense counterintelligence --

Counterintelligence Community
Department of Defense…

- SecDef
- USD-Intel
- CJS
- J2
- JFCOM
- CENTCOM
- NORTHCOM
- SOUTHCOM
- TRANSCOM
- PACOM
- EUCOM
- USMC

Defense Agencies (with organic CI capabilities)

- DIA
- NSA
- NRO
- NGA
- DTRA
- MDA
- DSS
- INSCOM
- 650th MI
- Tactical CI
- DASI-CDC
- NSA/CI
- NRO/CI
- NGA/CI
- DTRA/CI
- MDA/CI
- DSS/CI

Advises and Assists SECDEF (C & S)
on CI Matters
- Monitor & Evaluate CI Functional Areas
- Review & Evaluate reforms within DoD CI

Command & Control
DoD CI Community

Prepared by Mark L Reagan – 6 May 2002
Updated 1 June 2005
• As defined by EO 12333, counterintelligence is “information” and “activities conducted”… hence DoD counterintelligence is both knowledge and action --
  o Knowledge of adversaries’ intelligence activities and related threats
  o Action to hinder, frustrate, and exploit those activities

• Aligning with PDD-75, DoD counterintelligence transitioned from a functions-based to a mission-based approach… four core mission areas (see Appendix B) --
  o CI Support to Force Protection (FP), includes Combating Terrorism (CbT)
  o CI Support to Research & Technology Protection (RTP)
  o CI Support to Critical Infrastructure Protection (CIP)
  o CI Support to Information & Capabilities Protection (ICP), includes Countering Clandestine & Covert Threats (C3T)

• C3T often referred to as “classic counterintelligence” includes counterespionage (CE) activities… C3T today is more inclusive than previous notions of CE

---

Counterespionage that aspect of counterintelligence designed to detect, destroy, neutralize, exploit, or prevent espionage activities through identification, penetration, manipulation, deception, and repression of individuals, groups, or organizations conducting or suspected of conducting espionage activities

-- Joint Pub 1-02 (30 Nov 2004)

• Defense Counterintelligence Core Mission Areas & Counterintelligence Functions --

DoD Counterintelligence Mission Areas & Functions -- CI Matrix...

DoD Counterintelligence will develop, implement and maintain seamless, proactive capability and mechanisms to identify, understand, anticipate and prioritize threats within all four CI mission areas and to plan & execute integrated offensive & defensive CI activities that prevent, deter, neutralize, or exploit those threats

See Appendix A for additional information on the CI functions
• High level view of defense counterintelligence --

DoD CI... High Level View

**Counterintelligence (CI)**

- Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or international terrorist activities.

**CI-21**

- PDD 75
- National CI Strategy
- DoD CI Strategy

**Strategic Goals**

- Support SECDEF, Combatant Commanders, Service & DOD priorities & missions
- Maintain DOD advantages
- Protect the US against emerging threats
- Protect the safety & security of the United States through the prevention of WMD
- Achieve horizontal & vertical integration
- Respond to the emergence of developing threats

**DoD CI Mission**

- Detect, identify, assess, exploit, or counteract the current and future threats to DoD personnel, information, research, technology, and as defined by the SECDEF and in support of the DNI
- Protect information & capabilities and emerging threats to DoD...
- Maintain DoD advantages

**CI Functions**

- Collection
- Operations
- Investigations
- Analysis & Production
- CI Functional Services

**Event Driven**

- Requirement Driven
- Formal Requirements
- Ad hoc Tasking / RFIs

**Mission - Based Approach**

- CI Split to Force Protection
- CI Support to RTP
- CI Support to C3T
- CI Support to ICP / C3T

**Clients**

- SECDEN
- USD CY
- DoJ
- FBI
- CIA
- DNI
- NCIX
- JTFs
- Drive
- DoS
- CIFA
- JTFs
- Def Agencies
- Military Svcs
- Joint Staff
- Def Agencies
- JTFs
- DoS
- DNI
- Congress
- Field Agents

DoD Counterintelligence... more integrated, agile, and effective than ever before

- Prepared by Mark L Reagan, 12 Feb 2004
- Updated 11 Jun 2005

**CI Functions**

- Detect, identify, assess, exploit, or counteract the current and future threats to DoD personnel, information, research, technology, and as defined by the SECDEF and in support of the DNI
- Protect information & capabilities and emerging threats to DoD...
- Maintain DoD advantages

**CI Spt to Force Protection**

**CI Spt to ICP / C3T**

**CI Spt to RTP**

**DoD CI Mission Areas**

- CI Functional Services
- Analysis & Production
- Operations
- Collection
- Investigations

**CI Spt to Force Protection**

**CI Spt to ICP / C3T**

**CI Spt to RTP**

**DoD CI Mission**

- Detect, identify, assess, exploit, or counteract the current and future threats to DoD personnel, information, research, technology, and as defined by the SECDEF and in support of the DNI
- Protect information & capabilities and emerging threats to DoD...
- Maintain DoD advantages

**Defense CI... timely, responsive, and effective CI support to the warfighters is paramount**

- DoD CI executes its global mission throughout the spectrum of conflict... peace, crisis, pre-hostilities, war, and post-hostilities
- Defense CI... timely, responsive, and effective CI support to the warfighters is paramount
- DoD decision makers increasingly rely on and demand full-spectrum counterintelligence capabilities... counterintelligence is a key component of Effects-Based Operations (EBO)
- CI a unique and critical capability for the successful execution of DoD’s national security mission... an operational capability for defense decision makers and the warfighters

**“DoD Counterintelligence is a strategic capability, a weapon and a profession that is transforming to meet the complex threats of the 21st century”**

---

38 Roy L. Reed and Anthony D. McIvor, “Making the Case: Counterintelligence as a Strategic Asset,” *American Intelligence Journal* (Spring/Summer 2004), pg. 52.
Counterintelligence

In closing...

Most fundamental to counterintelligence -- as true today as ever -- is the need to ‘think the unthinkable.’ Yet this is one of the most difficult attitudes to instill and maintain because it runs contrary to human nature, especially in open societies like the United States. ... thinking the unthinkable is not easier, but it is just as critical to our national security.

As we proceed to face the counterintelligence threat of the 21st century, we are faced with a host of challenges: some new, others ancient and deeply rooted in human weakness, and some not yet even invented.

-- Honorable Richard Shelby (18 May 2001)
Chairman of the U.S. Senate Select Committee on Intelligence

In summary --

Counterintelligence, then, is a strategic instrument available to states to protect themselves and advance their interests in the struggle for power, wealth, and influence. ...But the end product, the mission of counterintelligence, is action—action to protect against foreigners and action to manipulate foreigners in the service of national goals.

Few counterintelligence practitioners get a chance to develop and implement plans to neutralize a whole [foreign intelligence] service, whether in a given area or worldwide. It takes vision, leadership, commitment, knowledge, and patience from the top of the counterintelligence establishment to do more than just arrest spies or run double-agent operations. Disrupting, neutralizing, or manipulating a foreign service does not bring counterintelligence practitioners public acclaim or even short-term private satisfaction, since it takes time, even years, to run its course...

Nevertheless, this is the mission—to understand the total foreign intelligence threat rather than fragments of it, and to exploit that knowledge to undermine foreign intelligence operatives for advantage. ...Counterintelligence, in all its aspects, is essential to the symbiosis that makes for first-class intelligence. 39

-- Roy Godson (1995)

• Early view as valid then as it is today --

Counterintelligence
A word from the wise…

Be generous with counterintelligence

-- Sun Tzu
circa 500 B.C.

Quote cited by Angelo Codevilla in Informing Statecraft: Intelligence for a New Century

Counterintelligence -- a strategic enabler and a national asset

“Counterintelligence is a never-ending necessity…”

Appendix A – The Traditional Counterintelligence Functions

Full array of active and passive (offensive & defensive) measures to protect friendly activities from adversary exploitation and manipulation

Introduction

- **Investigations**… catching traitors who spy for foreign intelligence services, or assist international terrorists, or commit other national security crimes

- **Operations**… wide range of actions to hinder, frustrate, and exploit foreign intelligence efforts and other foreign clandestine and covert activities damaging to national security

- **Collection**… obtaining information about foreign intelligence services, other clandestine and covert activities, as well as international terrorist groups/networks

- **Analysis & Production**… assimilating, evaluating, interpreting, and disseminating information of CI relevancy – a critical enabler providing insights into the threat

- **CI Functional Services**… other CI activities that support other intelligence or operational activities, including specialized defensive CI services such as Technical Surveillance Countermeasures (TSCM), polygraph/credibility assessment services, behavioral sciences, and cyber services, e.g., digital forensics, cyber vulnerability assessments, etc.

An overview of CI Investigations, Operations, Collection, and Analysis follows.

CI functions are interrelated -- operations can spawn espionage investigations; espionage investigations support collection and analysis activities; and collection and analysis are essential to the development of CI operations

---

40 TSCM are specialized techniques and measures to detect and nullify a wide variety of technologies used to obtain unauthorized national security information; protects against technical surveillance efforts – the use of electronic or mechanical monitoring devices or systems to obtain sensitive information without the knowledge or consent of the parties concerned.
**Counterintelligence Investigations**

**CI Investigations Defined...**

The systematic collection of information regarding a person or group which is, or may be, engaged in espionage or other clandestine intelligence activity, sabotage, or international terrorist activities conducted for, or on behalf of, foreign powers, organizations, or persons.

-- CI Community Lexicon, NACIC, June 2000

CI investigations seek to identify spies & others who commit national security crimes...

"The thankless and exhausting task of tracking down a traitor always seems much easier in retrospect than in prospect. The clues always seem so obvious -- but only after the hunt has caught its prey."

-- Markus Wolf, Former Director HVA ('58-'87)
East German Intelligence Service (Stasi)

**CI Investigations**

"Counterintelligence doesn't end with uncovering and finally catching the foreign spy [or] the US traitor. It ends only when there is enough hard evidence to arrest, successfully prosecute and convict the spy -- or turn him (or her) into a double agent working against his foreign handlers."

-- S. Eugene Poteat, CIA (Retired)
“You don’t catch spies by thinking like lawyers.”

-- Mark Hulkower, Assistant U.S. Attorney General (circa 1995)
Aldrich Ames Prosecution Team

CI Investigations

Espionage is a crime almost devoid of evidence...

-- Peter Wright, Former Asst Director MI5

Detecting, exploiting and defeating espionage
Counterintelligence Operations

CI Operations Defined...

Actions taken to “…to negate, confuse, deceive, subvert, monitor, or control the clandestine collection operations of foreign governments or agencies”

-- CI Community Lexicon NACIC, June 2000

Actions taken against foreign intelligence services to counter espionage and other clandestine intelligence activities damaging to national security

-- DoDD 5240.2

Activities taken to hinder multidisciplinary activities of foreign intelligence and security services, and to cause FIS to doubt the validity of its own analysis

-- AR 381-20

Counterintelligence Special Operations: direct engagement with known or suspected FIS through human source or technical efforts; includes offensive counterintelligence operations, counterespionage projects, defensive source programs, and investigative special techniques.

Focus of offensive counterintelligence is disruption of the adversary service...

------------------------

CI Operations As defined in JP 1-02...

Proactive activities designed to identify, exploit, neutralize, or deter foreign intelligence collection and terrorist activities directed against the Department of Defense (DOD).

-- DoD Dictionary (Joint Pub 1-02)

CI Operations are conducted to:

• Manipulate, disrupt, neutralize, and/or destroy the effectiveness of foreign intelligence activities;
• Recruit or induce defection of foreign intelligence officers and personnel;
• Collect threat information on foreign intelligence operations, modus operandi, intelligence requirements, targeting, objectives, personalities, communications, capabilities, limitations, and vulnerabilities;
• Provide information and operations databases to support decision makers;
• Provide counterintelligence support to clandestine human intelligence operations;
• Identify post, ongoing, or planned espionage;
• Support force protection, operations other than war, and peacekeeping;
• Acquire foreign intelligence espionage equipment for analysis and countermeasures development;
• Develop operational data, threat data, and espionage leads for future CI operations, investigations, and projects and develop the potential of these leads to enhance DoD security overall; and
• Support specific Chairman of the Joint Chiefs of Staff, DoD, and national plans.
Counterintelligence operations consist of obtaining and analyzing information on the adversary and then using it against him in accordance with the requirements of the situation and in light of our knowledge of his practices and psychological outlook.

An ideal counterintelligence system anticipates the enemy’s move, notionally satisfies his needs, and indeed operates a notional intelligence service for him.

"Countersabotage—A Counterintelligence Function" by Eric W. Tins, Studies in Intelligence, V7: 2 (Spring 1963), pg. 67

The use of double agents... a time-honored method both of deception and of counterespionage.

Double agents “can serve as excellent channels through which misleading information can flow to the enemy. So double agents serve both as collectors of positive intelligence and channels for deception.”

CI Operations

Sample of DA Objectives…

**Double Agents**

- Control adversary espionage and by doing so, in effect make them work for you
- Identify, neutralize, or suppress new agents and spies
- Secure information on the personnel and methods of the adversary service
- Secure access to adversary codes and ciphers
- Secure indication of the adversary’s intentions
- Lead, divert, or direct the enemy’s intentions
- Use DAs systematically as deception channels

Through the use of double agents, the U.S. intelligence community is able to identify hostile intelligence services:

- operatives and agents,
- “tradecraft”,
- electronic and photography eavesdropping capabilities, and
- sources and methods of operations.

In some cases, double agent operations have resulted the arrest of hostile intelligence officers…

Another goal… is to discourage hostile intelligence agencies from accepting “walk-ins”, who come to them offering their services.

---

Source: *Espionage*, Naval Investigative Service Command pamphlet, undated (circa 1989), Department of the Navy, p. 24

*Currently known as the U.S. Naval Criminal Investigative Service (NCIS)*
• Access Agents -- “another method of identifying and keeping track of suspected intelligence personnel is to recruit people close to suspects”

[CI] operators can seek out secretaries, janitors, chauffeurs, interpreters, neighbors, or friends and request that they pass on information about the target’s predilections and behavior.41

-- Roy Godson

• Penetration Operations42 are conducted to penetrate adversary intelligence services to --
  o Gain direct knowledge of operations against oneself, as well as to
  o Gain insights into the foreign intelligence services’ policy and other activities

---

Penetration:

the recruitment of agents within or the infiltration of agents, or the introduction of technical monitoring devices into an organization, group, physical facility for the purpose of acquiring information or influencing its activities.

[One of the most effective is known as a] Recruitment in Place (RIP): an official who overtly continues to work for his government and clandestinely provides information of intelligence value to a foreign government. ...[most often] connected with a foreign government’s intelligence service.

-- Counterintelligence Community Lexicon, NACIC, June 2000

Penetration… a time-honored espionage practice

Oh what a tangled web we weave...

---


Counterintelligence Collection

CI Collection

**Defined...**

The systemic acquisition of information concerning espionage, sabotage, terrorism, and related foreign activities conducted for or on behalf of foreign nations, entities, organizations, or persons and that are directed against or threaten DoD interests.

-- DoDD 5240.2 (27 May 1997)

Activities designed to acquire / collect / assimilate information on foreign intelligence services, terrorism, and related security threats. Information is collected from open sources, from liaison contacts, from indigenous sources, and from personal observation.


- CI collection feeds analysis and is used to formulate force protection and security policy, plans, & procedures, as well as assists intel collection operations and CI investigations & operations

- CI collection is the systematic acquisition of intelligence information using CI resources to answer validated CI collection requirements

- Collection is a continuous process driven by validated requirements

- Two key components of CI collection are *collection requirements management* (CRM) and *collection operations management* (COM)… two distinct but interrelated processes
  - The CRM process determines *what* will be collected and by *which* discipline
  - The COM process determines *how* a requirement will be answered and the *execution* of the collection activity

- CI collection is critical in addressing gaps in developing and updating a *common operating picture* (COP) on foreign intelligence threats and related activities

- CI collection supports operational planning, policy-making, decision-making, intelligence production, and the maintaining & updating of counterintelligence databases
Counterintelligence Analysis

CI Analysis

CI analysis is the function of assimilating, evaluating, and interpreting information pertaining to areas of counterintelligence proponency and responsibility. Information derived from all sources is considered and integrated in the analytical process.

-- Joint Pub 2-01.2 & DIA Reg 51-12

Identify the “threat” so decision makers can act decisively

CI Analysis

CI’s Critical Component...

Strategic analysis allows DoD CI to understand today’s risk environment. Long term analysis yields the requisite insights to predict threats to DoD assets in the mid term and distant future and relies on integrating the CI functions to “connect the dots.” A strategic analytical capability allows the Department to learn and use an adversary’s pressure points to influence its actions.

-- DoD Counterintelligence Strategy FY 2004 (16 Dec 2003)

CI analysis a critical enabler for Defense CI...
Astute analysis is a critical enabler for effective CI investigations, operations, collection, and most of the functional services...

-- Defense Counterintelligence Strategy
Appendix B – Four Core Defense Counterintelligence Mission Areas

- Counterintelligence Support to Force Protection, includes Combating Terrorism (CbT) --

CI Support to Force Protection (FP)

- **FOCUS:** CI activities that contribute to the protection of DoD personnel and their families from acts of terrorism, sabotage, and assassination. CI support extends to forces in CONUS and those stationed, deployed, or in transit abroad.

- **PRIMARY CONCERN:** combating terrorism (CbT), to include the activities that precede and support terrorist attacks—the activities of Foreign Intelligence & Security Services (FISS) in aiding or abetting terrorists are of particular concern. Also includes –
  - activities to detect & prevent impending sabotage & assassination against DoD personnel/assets;
  - activities related to the identification and mitigation of threats posed by organized criminal groups, illicit weapons dealers, and drug traffickers.

- **EMPLOYS:** full range of CI activities to identify and thwart clandestine and covert foreign elements that seek to harm US forces. It incorporates a significant portion of the base CI program, primarily at the field level.

- **INTEGRATION:** DoD CI activities in this mission area are integrated and synchronized with other efforts across the U.S. Government that contribute to FP and CbT, including physical and operational security, personal protective services, and intelligence activities.

- Counterintelligence Support to Research and Technology Protection --

CI Support to Research and Technology Protection (RTP)

- **FOCUS:** CI efforts to protect highly technical information, know-how, weaponry, and manufacturing processes associated with DoD research, development, technology, and evaluation (RDT&E) and designated acquisition programs; also includes CI activities to protect sensitive technical information and technologies on fielded systems.

- **PRIMARY CONCERN:** preventing the loss of critical program information (CPI) or materiel that could be exploited to degrade US combat effectiveness or technical superiority, achieve technological surprise, or damage US economic competitiveness.

- **EMPLOYS:** full range of CI activities to identify and counter foreign elements, insiders, and criminal elements that seek to acquire and exploit sensitive information or materiel associated with protected US defense technologies.

- **INTEGRATION:** CI activities in this mission area are executed in close cooperation with acquisition program managers, RDT&E site directors, the defense industrial community, and site security elements.
• Counterintelligence Support to Critical Infrastructure Protection --

**CI Support to Critical Infrastructure Protection (CIP)**

- **FOCUS:** CI efforts to protect infrastructures that DoD designates as critical to DoD mission success; includes physical and cyber components, within CONUS and OCONUS, and aligned with the Combatant Command responsibilities.
- **PRIMARY CONCERNS:** terrorism, cyber attack, sabotage, espionage, and related criminal activity directed against infrastructure elements critical to the accomplishment of US national security objectives.
- **EMPLOYS:** all aspects of CI to identify & counter foreign and domestic elements that seek to:
  1) acquire sensitive information concerning the critical infrastructures upon which DoD depends;
  2) exploit that information to disrupt the functions of that infrastructure.
- **INTEGRATION:** CI activities in this mission area are executed in cooperation with facility managers; industry, military and site security elements; and local, state & federal law enforcement.

• Counterintelligence Support to Information Capabilities Protection (ICP), includes Countering Clandestine and Covert Threats (C3T) --

**CI Support to Information & Capabilities Protection / Countering Clandestine & Covert Threats**

- **FOCUS:** CI activities most closely associated with “classic counterintelligence” as noted in the 1999 Mission Area Analysis of DoD Counterintelligence.
  - In the past often referred to as “Counterespionage” or “CE” – this mission area is today more inclusive than previous notions of counterespionage.
  - Includes countering denial & deception and influencing the actions of adversaries & allies.
- **PRIMARY CONCERN:** protection of US military capabilities (including intelligence & CI capabilities/activities), plans, and operations from espionage and insider threats.
- **EMPLOYS:** integrated CI campaigns, centrally coordinated sets of collection, analysis, investigations, and operations focused on defeating global activities of designated Foreign Intelligence & Security Services (FISS) and/or terrorist groups & networks. Includes counter-espionage, investigations of anomalies, and the unauthorized disclosure of classified information.
- **INTEGRATION:** this mission area includes much of the CI base program activity at the strategic and operational levels within the DoD CI community. Incorporates majority of the investigative and operational activity of Defense CI unless or until a linkage to another mission area is clearly established and may incorporate efforts related to FP, RTP, and CIP.
Counterintelligence
One final perspective...

...the practical criticism of ambiguity.

-- James Jesus Angleton
CIA’s Chief of Counterintelligence
1954 to 1974

Counterintelligence... a wilderness of mirrors

“People who think we don’t need to be vigilant about counterintelligence... are wrong”

-- George Tenet, Former DCI