A Guide to Counterintelligence

Michael Ellmer ⋮ 17-22 minutes

---

1. Why is counterintelligence important?

Counterintelligence (CI) is an essential discipline and practice within the intelligence community and national security spheres. In fact, it is essential for the private intelligence sector as well, in the corners that lodge various forms of intelligence value, ranging from raw data and trade secrets, to defence contracts and the cyber infrastructure that houses them.

However, akin to the definition of intelligence, and the intelligence cycle – counterintelligence joins its relatives in traversing the strange thickets of conceptual debate. There is no universally agreed upon definition of counterintelligence – it has different meanings to different agencies and nations. Because of this, the question of *why* counterintelligence is important correlates to how it is viewed.

1.1 Counterintelligence defined

For example, here are a few similar yet different definitions of CI:

“information collected and analyzed, and activities undertaken, to protect a nation (including its own intelligence-related activities) against the actions of hostile intelligence services.” – Abram Shulsky and Gary Schmitt (source)

“Counterintelligence is traditionally understood to include operations designed to block, disrupt, or destroy the intelligence operations of an adversary.” – Jennifer Sims (source)

“information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.” – the United States government (source)

“Counter-intelligence is defined as those activities that identify the threat to security posed by hostile intelligence services or organisations or by individuals engaged in espionage, sabotage, subversion, terrorism or other non-traditional threats.” – the United Kingdom Ministry of Defence (source)

1.2 Narrowing the conceptual focus

For this guide, we will look at counterintelligence through the lens of scholar Hank Prunckun, who rests his theory of counterintelligence on seven assumptions:

1. **Operational Surprise:** counterintelligence supports general intelligence functions, which enables them to achieve operational surprise.
2. **Data Collection:** opposition forces will collect data on intelligence agency’s operations. If an opposition force does not have the intent of collecting this data, a counterintelligence program is not justified.
3. **Targeting:** the opposition will focus data collection efforts on the operational capacity of an agency and the entities it protects:
    - Agency structure
        - Legal
        - Constitutional
        - Chain of command
        - Personnel

    - Sphere of operations and influence
        - Geographic
        - Economic
        - Sociopolitical
    - Current capabilities
    - Future intentions
4. **Resources:** counterintelligence programs require resources, including physical staff and specialised equipment.
5. **Paradox of Fiction:** the experience of being convinced something is true and exhibiting associated emotions despite it being an illusion (an offensive counterintelligence practice.)
6. **Operational Failures:** wherever there is risk, there is the chance for failure.
7. **Analysis:** counterintelligence needs to have an analytical foundation (hence why it is not a purely "put documents in a safe" function, i.e. security).

These assumptions rely on the principles of deterrence, detection, deception, and neutralisation to counteract the opposing party's information-gathering activities. The reason for opposition data collection is irrelevant, as these principles apply equally to any motive, whether it be for intelligence gathering, subversion, sabotage, terrorism, weapons proliferation, or competitive advantage. This theory broadens counterintelligence to be relevant not only to the government, but to the private sector as well. (source)

Further, Prunckun breaks down the anatomy of counterintelligence into two distinct yet interconnected parts: counterintelligence (defensive) and counterespionage (offensive). (source)

1.3 Defensive vs. offensive

Counterintelligence and counterespionage do not hold the same definition, contrary to popular thought. Within Prunckun's framework, one is a defensive practice and concerned with denial, and the other is offensive and concerned with deception.

Defensive (counterintelligence – denial)

- Deterrence and detection
- Related to security, yet not security (in a strict sense)
- Prohibits enemy access to information and data collection
- Discourages an enemy from conducting penetration operations
- Security
    - Physical
    - Information
    - Personnel
    - Communications
- Detecting an "event of concern" (hostile penetration or hostile attempt at collection)

Offensive (counterespionage – deception)

- Misleading the opposition
- Concealing an active penetration operation
- Drive opposition to waste resources
- Neutralising the opposition's intelligence collecting capability
- Sow discord or reduce confidence within an oppositions agency

2. How do you do counterintelligence?

Before moving away from the conceptual aspects of counterintelligence, it is beneficial to briefly mention its function as a sort of counterpart to "positive intelligence", for lack of a better term.

What this means is that each discipline of intelligence – HUMINT, SIGNIT, OSINT, etc – has a counterintelligence function on its opposite end. This is important, as each collection method has its own set of counterintelligence practices.

In addition, different agencies, organisations, governments, companies, etc., will have their own specific tactics, techniques, and procedures as well.

To prevent getting too entangled in the vastness of these differences, we will summarise general counterintelligence practices and cover highlights from a few of the major collection disciplines.

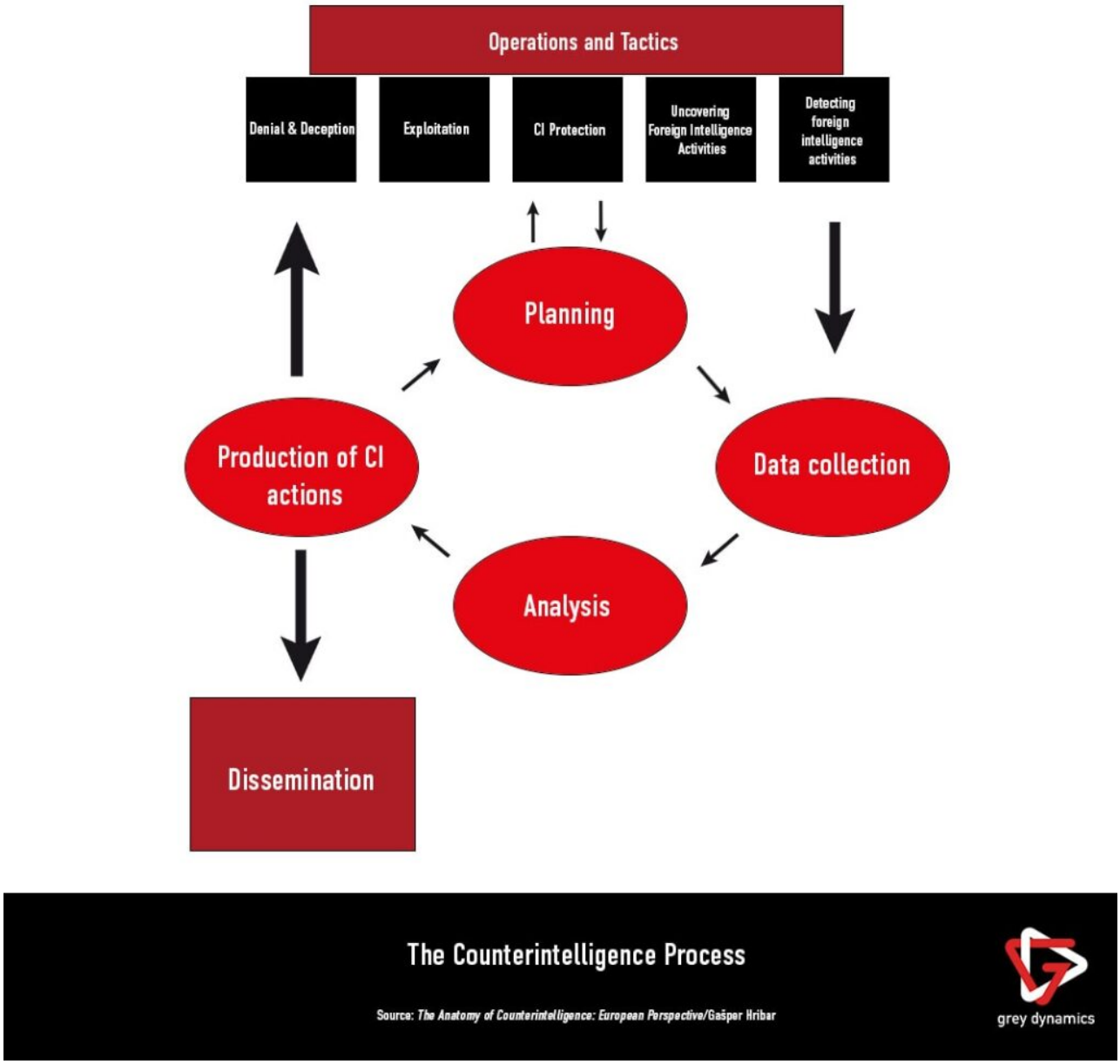
2.1 General counterintelligence tradecraft

The counterintelligence process

Similar to the intelligence cycle, we can break counterintelligence down into a process. Scholar Gašper Hribar breaks this process into four steps (source):

1. **Planning:** defining goals and establishing intelligence priorities.
2. **Data collection:** collecting information through all-source disciplines.
3. **Analysis:** data evaluation, analytical methods.
4. **Production & dissemination:** report drafting, briefing and dissemination to customers.

Similarities with the intelligence cycle aside, the fundamental difference is within the direction and final product, which can cause counterintelligence actions, directed at implementing defensive solutions or offensive actions – defensive counterintelligence or offensive counterespionage, to draw back on Prunckun.



Operational security (OPSEC)

OPSEC is paramount in virtually any sensitive environment, but detrimental for counterintelligence.

The U.S. government defines OPSEC as a “Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities.” (source) That process is five steps:

1. Identification of critical information
2. Analysis of threats
3. Analysis of vulnerabilities
4. Assessment of risks
5. Applications of countermeasures

This process is not strictly for government employees or members of the intelligence community. It is just as important in the private sector as well, especially when there are trade secrets on the line, or the risk of economic or industrial espionage from a competitor or hostile threat actor.

2.2 All-source tradecraft

- **Double/penetration agents:** this includes detecting and deterring adversary agents (defensive) and cultivating or handling your own, as a way of neutralising or lessening your adversary's intelligence collection capabilities.

- **Covert surveillance:** covert observation and tracking of "people, objects, facilities, or anything else deemed of value by the (intelligence) service." (source)
- **Technical surveillance:** surveillance aligned with technical collection methods (i.e. SIGINT, COMINT). This includes through the utilisation of electronics, communication equipment, and video surveillance.
- **Counter surveillance:** deterring, preventing, and exploiting an adversaries' attempts at surveillance.

3. Counterintelligence tips and tricks

Counterintelligence is a diverse field with a myriad of strategies ready for implementation. As a base level practitioner, there is an assortment of noteworthy skills that are beneficial to possess.

- **Situational awareness/attention to detail:** situational awareness and attention to detail go hand in hand with counterintelligence. For a basic practitioner, these skills highly apply in any relevant workplace. For example, being aware of your co-workers' baseline, and noticing if there are any deviations from it. Unplanned life circumstances, tragedies, and ideological shifts are subtle changes that could mean someone is vulnerable to adversaries, or prone to becoming an enemy double agent (applicable in professional environments where there is intelligence value to be gained).
- **Specialised education and training:** learning about the threats to your professional environment and developing an awareness of counterintelligence concepts. This includes not only threats, but internal security and sensitive material handling procedures.
- **Vetting:** for people in hiring positions, vetting is a crucial practice to help identify possible counterintelligence threats early on. Vetting itself is its own topic, but this can include background checks, interviews, and social media audits of prospective employees.
- **Internal monitoring:** having monitoring capabilities around the professional environment is a key way to both deter and detect. This can include physical security, cameras/CCTV, alarms, and other forms of internal security.

4. Common mistakes in counterintelligence

- **Poor OPSEC:** poor OPSEC leads to fractures in security and opens an entity up to the intelligence actions of an adversary.
- **Improper education:** this includes personnel not having adequate training in OPSEC, organisational procedures, and safe handling of sensitive materials.
- **Failure to report:** specifically, failure to report individuals who have a noticeable shift in behaviour or signal red flags.
- **Weak vetting:** improper background checks and poor vetting procedures is a significant risk to organisational security.
- **Complacency:** complacency can mean many things for counterintelligence. One example is having a narrow view of what makes a threat, i.e. directing efforts to protect an organisation from external penetration when there is an equal internal risk.

5. Tools and resources for counterintelligence

5.1 Courses

- Counterintelligence Awareness and Reporting Course for DOD
- Certified Counterintelligence Threat Analyst (McAfee Institute)
- Counterintelligence 101 Certification Crash Course (udemy)

- Introduction to Technical Surveillance Counter Measures – Electronic Bug Sweeps (udemy)
- Counterintelligence Courses and Briefings – Centre for Counterintelligence and Security Studies
- Cyber Counterintelligence Tradecraft – Certified Cyber CounterIntelligence Analyst (Treadstone 71)

5.2 Books

- Counterintelligence Theory and Practice (Amazon)
- To Catch a Spy: The Art of Counterintelligence (Amazon)
- Vaults, Mirrors, and Masks: Rediscovering U.S. Counterintelligence (Amazon)
- Thwarting Enemies at Home and Abroad: How to Be a Counterintelligence Officer (Amazon)
- Dirty Tricks or Trump Cards: U.S. Covert Action and Counterintelligence (Amazon)
- The Anatomy of Counterintelligence: European Perspective (Amazon)

6. Frequently asked questions about counterintelligence

Why is counterintelligence important?
Conducting intelligence without having a strong counterintelligence program puts an agency, organisation, or nation at a great disadvantage over their adversaries. As advantage is a component of intelligence operations and strategy, counterintelligence helps gain or preserve that, when done correctly. In addition, CI drives the mechanisms that protect national secrets, which in return protects national security. In the private sector, counterintelligence helps preserve sensitive information that can give a competitor an advantage, or open your organisation up for attack.

How can organisations stay current with the latest threats and trends in counterintelligence?
This will vary based on the organisation and its capabilities. Specifically, for the private sector, having a dedicated intelligence team is a resource-heavy way. At an individual level, continuing education and staying informed with current affairs related to your industry or open-source information regarding threats that may target your organisation are both places to start.

7. Advanced counterintelligence techniques

7.1 Cyber counterintelligence

Cyber counterintelligence (CCI) is a quickly evolving subelement of the counterintelligence discipline, like how cyber operations are becoming increasingly enmeshed with intelligence. Practically, CCI is a way for actors to secure (defence) and advance (offense) their cyber interests. (source) Although CCI is growing in scholarship and awareness, it is still a rather niche field that does not receive as much attention as other CI practices.

Scholars Petrus Duvenage and Sebastian von Solms have developed a useful matrix with CCI practitioners in mind. It covers both defensive and offensive modes.

1. **Passive-defence mode**: physical and cyber security systems that deny opposition access.
2. **Active-defence mode**: active collection, surveillence, human intelligence, prior opposition practice.
3. **Passive-offensive mode**: Honey-pots, selective information exposure.
4. **Active-offensive mode**: disinformation campaigns, covert action, offensive cyber-operations.

And, like normal intelligence, each axis on this matrix is broken into three levels: strategic, operational, and tactical-technical.

7.2 Covert action

When it comes to the intersection of counterintelligence and covert action, Roy Godson says it best: “As with counterintelligence, history is replete with examples of the advantages that accrue to states

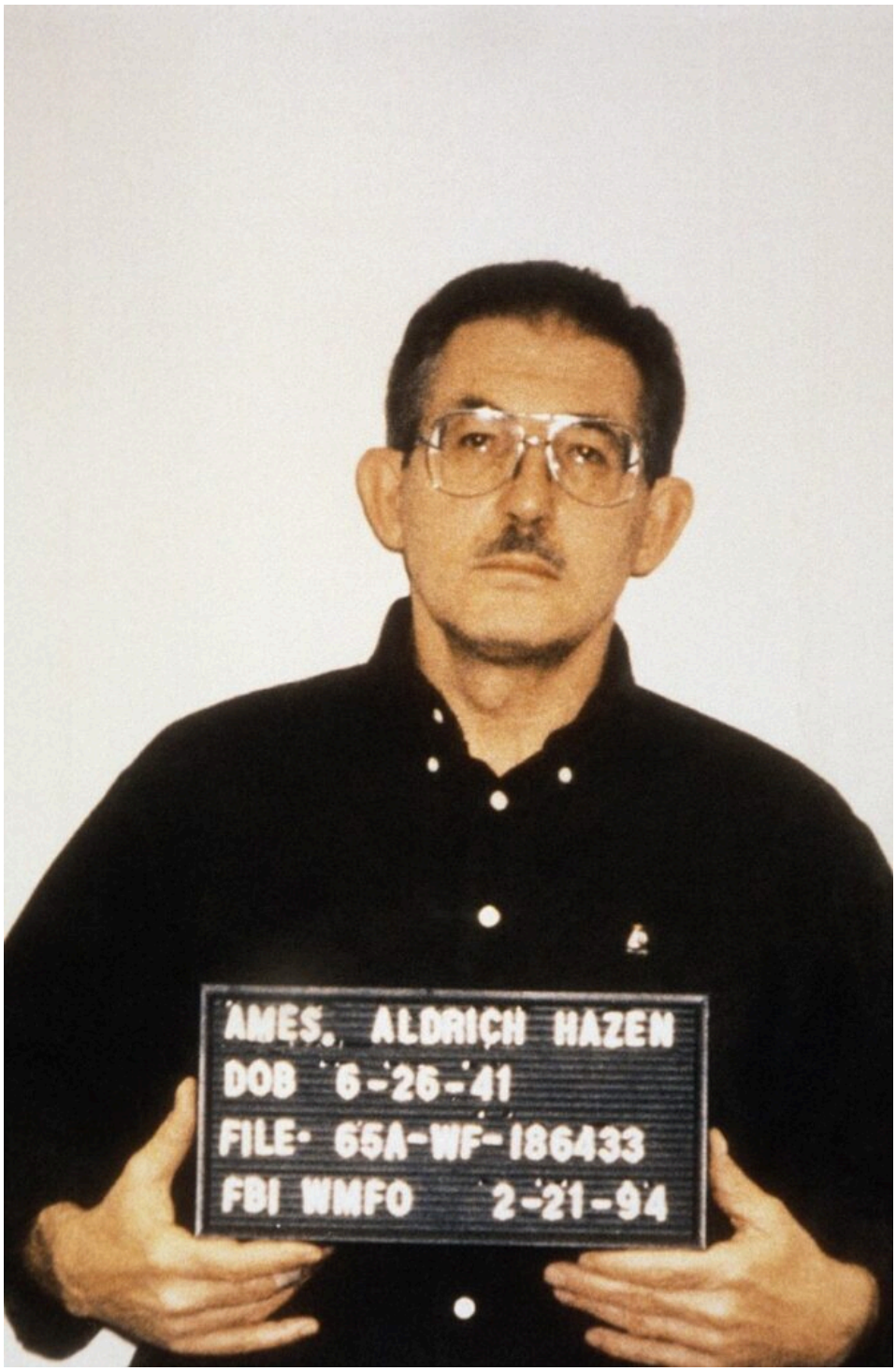
that blend an effective covert action capability into their overall policies, and of the problems besetting those that do not." (source) By and large, covert action and counterintelligence are both essential tools wielded in the protection of national security.

As it relates to counterintelligence, covert action operations are generally concerned with espionage, sabotage, and subversion (ESS). In part, protecting one's own organisation or agency from ESS is itself a defensive CI function. However, the offensive side would fall under covert action. Further, ESS can be conducted in different ways depending on the INT – HUMINT driven ESS will look different than a cyber-operation, yet they share the same foundation.

8. Counterintelligence case studies

8.1 Aldrich Ames

Aldrich Ames is one of the most prolific examples of a counterintelligence failure in U.S. history. From 1985 to 1994, Ames lived a double life as a CIA counterintelligence officer and a Soviet agent. Coencidentaly, Ames was a specalist on Soviet affairs, and spent his early career targeting KGB officers for recruitment. In 1985, Ames volunteered to be a KGB asset for substantial payments. There were a few indicators in his personal life, that he was vulnerable to recruitment, such as alcoholism and extramarital affairs. In May 1993, the FBI opened a case after recieving information regarding Ames' unexplainable wealth gains. An almost year long investigation resulted in his arrest and further guilty plea in April 1994. Ames was sentenced to life in prison without the possibility of parole. His time as a Soviet agent resulted in the executions of multiple U.S. citizens overseas. (source)



Aldrich Ames' mugshot (Image: wikicommons)

8.2 Ana Montes

Ana Montes is another U.S. double agent who was recently released from incarceration. Montes was once the Defense Intelligence Agencies top Cuban analyst, yet harbored sympathy for their cause. Her personal ideological leanings drove her to become a Cuban agent, which was ideal given her prime access to some of the nations most sensitive defence intelligence. Contrary to Ames, money was not a driver. Montes is an example of the power of ideology, and how it can result in some of the most steadfast agents. She was eventually caught and prosecuted, pleading gulilty in 2002 and recieving a 25 year prison sentence. (source)

CIA Director George Tenet (left) awards Ana Montes a Certificate of Distinction, the third highest national-level intelligence award. From 1997. (Image: wikicommons)

8.3 Byzantine Hades

Byzantine Hades is an example of a CCI operation – both a counterintelligence failure and success for the U.S. in the early to mid 2000s. In essence, Byzantine Hades is the codename for an array of Chinese advanced persistent threats that over the course of a few years, hacked into numerous Department of Defense systems through spearfishing attacks. As a result, the Chinese threat actors stole massive quantities of sensitive information, including schematics for the F-35 fighter jet, which was used to help their own next generation fighter jet program. This economic espionage resulted in millions of dollars in damage to DoD systems, and thousands of compromised accounts. It was kept private until the WikiLeaks scandal and further leaks from NSA whistleblower Edward Snowden. (source)

9. Conclusion

Counterintelligence is a vital counterpart to positive intelligence, and an absolute necessity for the perservation of national security. Its relevance crosses beyond the government sector, and into the private as well. As intelligence is shaped by the advancements of society, so to does counterintelligence ride the ebb and flows of history, leaving valuble lessons in its wake, and generating thought-provoking questions about what it will look like in the future. Legendary CIA officer James Jesus Angleton describes it best: “A wilderness of mirrors”.