Global Security Studies, Fall 2014, Volume 5, Issue 4

United States Counterintelligence

Benjamin York
Campbell University
Buies Creek, NC 27506
bbyork0506@email.campbell.edu

Abstract

Counterintelligence is one of the most vital areas of the modern United States intelligence system. The main goal of counterintelligence efforts is to prevent enemy states and organizations from stealing classified information from the intelligence community. This involves detecting spies inside the US intelligence community and creating a plan of action to apprehend these spies. Several improvements have been made to the modern intelligence system to prevent penetration of enemy spies, but some issues still exist because no system is perfect. As a result, the US intelligence system is still being modified to create a secure environment from enemy threats of espionage.

Key Words: Counterintelligence, Counterespionage, Espionage, FBI, CIA

Introduction

Sun Tzu, one of the greatest military strategists that ever lived, wrote in *The Art of War* "all warfare is based on deception" (Tzu, 11). This concept could not be applied better to any other area than counterintelligence. In fact, counterintelligence is so secretive that it could be described as completely deception based. Counterintelligence primarily consists of human intelligence issues, including discovering foreign agents in the US intelligence system and then choosing the appropriate plan of action to apprehend these foreign agents. However, counterintelligence is much more complicated and problematic than previously described. Several problems in the intelligence field exist as a direct result of counterintelligence, with no solutions having complete effectiveness in solving the issues.

Background

In order to understand the problems presented by counterintelligence, one must first understand the exact nature of counterintelligence. Mark M. Lowenthal, a PhD recipient in history from Harvard University, has thirty-six years of experience with the intelligence community by serving in the Congressional Research Service, the State Department, the House Intelligence Committee, and the Central Intelligence Agency. According to Lowenthal, Executive Order 12333 defines counterintelligence as, "'information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect' against espionage and other activities carried out by foreign states or non-state actors" (Lowenthal, 163). A crucial area in understanding counterintelligence is that it branches out into all areas of intelligence and is not a separate part of the intelligence process. Counterintelligence can be broken down into three fields: collective, defensive, and offensive counterintelligence. Collective counterintelligence involves gathering information against an enemy nation's collection methods and capabilities.

Defensive counterintelligence consists of preventing an enemy's agents from penetrating the home nation's (United States') agencies. In contrast, offensive counterintelligence consists of attempting to turn enemy agents into double agents or giving them false or misleading information once they have been identified in the hopes that these agents will report the information back to their home nation (Lowenthal, 163). Furthermore, there are numerous activities that counterintelligence is involved in. Paul Redmond, a CIA officer who primarily worked with counterintelligence issues, listed a variety of these activities. "Redmond's list includes counterespionage (countering penetrations of one's service), asset validation (confirming the bona fides of human intelligence sources), disinformation (putting out false information to support penetrations), and operational tradecraft" (Lowenthal, 163-164). In other words, the foundation of counterintelligence is made up of those areas previously described.

Common Issues

The most fundamental problem in counterintelligence is that counterintelligence officers are not likely to have compelling evidence to successfully prove that there has been successful enemy penetration of the intelligence community (Lowenthal, 170). More times than not, this theory can be found in US intelligence agencies. Most counterintelligence issues are targeted at intelligence agencies and organizations because they are the most valuable intelligence targets for stealing classified information (Lowenthal, 163). One of the most detrimental counterintelligence difficulties in American intelligence agencies is that the agencies trust the people who work there because they have gained the necessary clearance (Lowenthal, 170). The reasoning behind this concept is that employees are required to go through an extremely difficult process in order to become hired. According to Lowenthal, "The vetting process for applicants includes extensive background checks, interviews with the applicants and close associates, and, in the United States at least, the use of the polygraph at most agencies" (Lowenthal, 164). What Lowenthal means is that employees who work at American intelligence agencies must undergo several various types of tests and trials before they can be hired. Lowenthal also goes on to suggest that the espionage problems in the American intelligence agencies arise from familiarity with co-workers. This false sense of security allows for employees to refuse to accept the notion that one of their co-workers is really working against them. An example of this concept can be found in the detection of Robert Hanssen. Hanssen was able to avoid detection for a lengthy period of time because the FBI concentrated on searching for a CIA officer as the spy in the US intelligence system when the spy was really one of its own. The FBI was convinced that the spy had to be operating out of another agency because it trusted its own agents (Lowenthal, 171).

The reverse effect of too much trust can be found in unwarranted suspicion. Unwarranted suspicion presents a problem in counterintelligence because an agency can act on irrelevant information and, by doing so, waste time looking for a mole that is not really there. Lowenthal illustrates this concept by drawing attention to James Angleton, the man presiding over CIA counterintelligence cases during much of the Cold War. Angleton was under the impression that a Soviet agent had penetrated the CIA and wasted several years and countless resources looking for this agent, who was never found (Lowenthal, 171).

CIA/FBI Conflict

Another main concern that undermines US counterintelligence efforts is the conflict between the CIA and the FBI. This conflict between the CIA and the FBI primarily arose from J. Edgar Hoover's deep hatred and distrust of the CIA. Hoover was the director of the FBI for several years and established almost what one could call a precedent for the FBI to hate and distrust the CIA, which the CIA mirrored in its negative views of Hoover and the FBI. Another source of friction between the CIA and the FBI can be found in their differing views about how to handle counterintelligence issues. On the one hand, the CIA tries to use discovered spies for counterespionage and offensive counterintelligence against the spies' home nations, whereas on the other hand, the FBI wishes to expose spies and prosecute them in federal courts on charges of espionage (Lowenthal, 171). This explanation displays the friction between the two agencies because the goals of one agency contradict and completely eradicate the goals of the other agency. An example of the damaging effects of mistrust between the CIA and the FBI in allowing a foreign agent to go undetected can be found in the case of Aldrich Ames. Lieutenant Colonel Crane, a professor and Chairman of the United States Army's Judge Advocate General's School in Charlottesville, Virginia, illustrates this idea and provides the answer to the question of how Aldrich Ames was able to avoid detection for so long. Crane states, "In the short term, the conflicting missions of the CIA and the FBI resulted in an ineffective initial investigation, and in the long term, the reason for the delay in the detection of Ames was due to a history of mistrust between the FBI and the CIA" (Crane, 27).The FBI eventually narrowed the list of suspects down to Ames because of his drinking habits and suspicious lifestyle (Crane, 29). This mistrust had a major negative effect on US intelligence collection inside the Soviet Union and Russia from the mid 1980's through the early 1990's. As a result, barely any effective human intelligence was collected on the Soviet Union and Russia during this time frame (Crane, 27).

Big/Little Counterintelligence

One of the most disputed issues in US counterintelligence is uncovering the information that discovered spies have learned since penetrating the agency and their motives behind going after the information they chose to steal. There are two classifications of counterintelligence dealing with this issue: big counterintelligence and little counterintelligence. Big counterintelligence is the action of finding out why a spy went after certain information in order to understand how the spy penetrated the agency and his or her intended goals. In contrast, little counterintelligence consists of finding out information such as how the agency was penetrated, how long the spy was undercover in the agency, who is directing the spy, and which information the spy has leaked to the opposition (Lowenthal, 172). In other words, big counterintelligence deals with the question of why the spy penetrated the agency, while little counterintelligence deals with the questions of what information has been compromised, how long the agent was under cover, and who is pulling the strings.

Damage Assessment

Regardless of the agency in question, after a spy has been caught, the agency must initiate a damage assessment in order to acquire a complete picture of the intelligence that has been compromised by the enemy (Lowenthal, 173). The reason why this action is of so much

importance is because intelligence leaked to the enemy is no longer relevant and can no longer be used by the United States. Once the damage assessment has taken place, the spy is then questioned by a prosecutor in the presence of the spy's attorney; this is of significant importance to the spy because the more the spy cooperates, the better his or her criminal sentence generally is. However, some of the most serious problems with interrogating captured spies are making sure the spy is being honest about the intelligence that has been compromised and for the intelligence officers involved to not use the captured spy as an excuse for compromised intelligence that the spy did not have access to (Lowenthal, 173). Intelligence officers should be cautious of the spy's responses just in case the spy is using the interrogation to mislead the intelligence officer. The interrogation also needs to remain on the information that the spy had access to because there may be another spy with similar access clearance who has not yet been exposed. Again, the Ames and Hanssen cases could be examples of this concept (Lowenthal, 173).

External Indicators

The US uses external indicators as part of counterintelligence to prevent espionage. External indicators of problems could be, "the sudden loss of a spy network overseas, a change in military exercise patterns that corresponds to satellite tracks, or a penetration of the other service's apparatus that reveals the possibility of one's own service having been penetrated as well" (Lowenthal, 169). The US could use these activities as indicators that a foreign agent has penetrated the intelligence community and is on the inside. To illustrate the importance of this concept, Lowenthal states that the intelligence that could be gathered by infiltrating an enemy agency (or intelligence a US agency could give up if infiltrated) is, " An opponent's human intelligence capabilities and targets, strengths, weaknesses, and techniques; the identity of clandestine service officers; an opponent's main areas of intelligence interest and current shortfalls; possible penetration of one's own service or other services; possible intelligence alliances; and sudden changes in an opponent's human intelligence operations, new needs, new taskings, changed focuses, and a recall of agents from a specific region" (Lowenthal, 169). So what exactly is the significance of all of these areas? All of these areas directly relate to espionage, which in turn directly relates to counterintelligence because espionage is one of the primary needs for counterintelligence.

Counterespionage

Counterespionage is another tool in counterintelligence that the United States uses to combat espionage. According to *The Encyclopaedia Britannica*, the definition of counterespionage is, "espionage directed toward detecting and thwarting enemy espionage." So why is counterespionage so important in relation to counterintelligence? Reginald Bullock, a Major in the United States Air Force, writes, "Espionage makes counterespionage necessary. United States counterespionage initiatives lead to the capture of [enemy] agents" (Hastedt, 120). This idea is one of the major goals that counterintelligence serves to achieve because a significant part of counterintelligence consists of capturing enemy agents that have penetrated the intelligence community. Often times, counterespionage uses dangles to draw out supposed spies that are intentionally placed "in front of a foreign service to see how they react" (Lowenthal, 170). In other words, one way the intelligence community uses counterespionage to

catch spies is by using baits to read the responses of suspected foreign agents. Sometimes offensive counterintelligence can be used in counterespionage in dealing with foreign agents. Counterespionage can be used to identify foreign agents and feed them false information that they will relay back to their home countries to confuse their intelligence analysts. Another strategy that is sometimes used is trying to recruit foreign agents as double agents to spy on their home nation for the United States. However, the real danger comes from triple agents who have been turned again by their home nation after first being turned by the United States (Lowenthal, 170). The idea of using double agents is one of the more common aspects of counterespionage, yet, as noted above, has potential to be one its most substantial setbacks. This issue is one of the central unanswered problems that today's intelligence community faces.

Hiring Process

Defensive counterintelligence contains several safeguards to protect the US intelligence community from espionage. The first of these safeguards is that every intelligence agency has a system of processes and checks designed to eliminate questionable applicants. US intelligence agencies do not just hire anybody and reflect this philosophy through the job application process. In the United States, the job application process involves a personal interview, a thorough background check, and using the polygraph on prospective employees (Lowenthal, 164). The use of the polygraph will be discussed more thoroughly later on. In addition to prospective employees, US intelligence agencies also evaluate current employees to look for potential signs of disloyalty and their likeliness of being turned. "Changes in personal behavior, marital problems, increased use of alcohol, suspected use of drugs, increased personal spending that seems to exceed known resources, and running up large debts may be signs that an individual is spying or susceptible to being recruited or volunteering to spy" (Lowenthal, 166). If a US intelligence agency has reason to believe that there may be a mole on the inside, these are the indications it will use to begin its search. Again, the Ames case is an example of this concept.

The most effective defensive counterintelligence strategy in use in the United States is the use of the polygraph. Two types of polygraphs exist in today's intelligence agencies; the lifestyle polygraph is used for questioning individuals about personal behavior, and the counterintelligence polygraph is used for asking questions about classified information (Lowenthal, 165). Lowenthal provides insight as to what exactly the polygraph is and various problems with its use:

> The polygraph, sometimes mistakenly referred to as a lie detector, is a machine that monitors physical responses (such as pulse and breathing rate) to a series of questions. Changes in physical response may indicate falsehoods or deceptions (Lowenthal, 164-165).

The polygraph is less effective when dealing with counterintelligence issues because the questions normally asked are general questions, resulting in less difficulty avoiding the actual questions in the responses. For example, Larry Wu-tai Chin and Aldrich Ames are two individuals who passed polygraph tests and were convicted of espionage against the United States (Lowenthal, 165).

One significant problem in the modern US intelligence community is that not every agency uses the polygraph when evaluating employees. "The CIA, DIA, NRO, and NSA all use

polygraphs; the State Department and Congress do not" (Lowenthal, 165). Lowenthal also goes on to state that the FBI did not use the polygraph test until after the Hanssen case (Lowenthal, 165). This is a problem for the intelligence community because the polygraph is one of the most effective tools at the United States' disposal in combating espionage.

Policy Changes

In addition to the tools and strategies in counterintelligence, the US has developed policy changes in counterintelligence in order to defend against espionage. On May 4, 1994, President Clinton created "Presidential Decision Directive 24" on the issue of counterintelligence (Crane, 36). Presidential Decision Directive 24 was signed into law on October 14, 1994 and was designed to allow the National Security Council to create a coordinated counterintelligence structure. The two initiatives dealing with counterintelligence in Presidential Decision Directive 24 were policy coordination and integration and cooperation (Crane, 36). The goal of the directive was that "this new structure [would] ensure that all relevant departments and agencies have a full and free exchange of information necessary to achieve maximum effectiveness of the US counterintelligence effort, consistent with US law" (Crane, 36).

In addition to Presidential Decision Directive 24, more modern changes have been made to the intelligence system to increase productivity and protection of information. The US now uses a classification system to divide the intelligence field into compartments. The division of the intelligence field into compartments is a safety measure to prevent an employee who has gained clearance from unlimited access to all intelligence (Lowenthal, 167). Before the terrorist attacks on September 11, 2001, access to US intelligence was on "a need to know" basis (Lowenthal, 167). The reasoning behind this policy was so that an employee's knowledge and access to intelligence was limited to the area in which he or she was working as a defense against espionage. An example of this concept would be that someone working with signals intelligence (or SIGINT) would not have abundant and unrestricted access to human intelligence information (or HUMINT). DNI McConnell changed this policy during his term by initiating "a responsibility to provide" instead of the "need to know" basis that was previously used (Lowenthal, 167). But what exactly does "responsibility to provide" mean? It means, "Officers and agencies now [will] be evaluated by the degree to which they actively seek to share intelligence" (Lowenthal, 167). This new system is effective because it reduces the damage caused by one source leaks but has its drawbacks in the fact that it can hinder analysts by denying them access to a compartment necessary for their assignment (Lowenthal, 167). These policy changes have greatly improved US counterintelligence efforts but are still being polished due to their drawbacks and incomplete effectiveness.

Policy Recommendations

Counterintelligence is a much deeper and problematic subject matter than it appears at surface level. Because the United States is such a powerful nation, the idea that one of its agencies has been penetrated would be difficult for an employee in that agency to grasp. This idea is only natural, considering the rigorous and numerous aspects of the job application process that employees must undergo before being hired. However, any suspicious activity inside an intelligence agency should be reported to an intelligence officer as a precautionary safety measure. As far as the conflict and friction between the CIA and the FBI is concerned, the only

course of action that the United States can take is to promote sharing of intelligence and increased interagency cooperation between the two. This concept is not just limited to these two agencies but is also applicable to all US intelligence agencies. Furthermore, the United States is certainly not hurting itself by placing external indicators and counterespionage measures, such as feeding foreign agents false information, as top counterintelligence priorities to defend against espionage. As far as internal protections are concerned, the United States should continue to require prospective employees in the intelligence field to go through strict and rigorous applications, including the use of the polygraph, in order to defend against penetration of foreign agents. However, the most important fact that can be learned from this research is that no policy is perfect; every plan has its solutions as well as its drawbacks. The US intelligence community needs to continue to attempt to polish and improve the current intelligence system in order to maximize effectiveness and minimize drawbacks.

Conclusion

Counterintelligence is one of the most important areas of any intelligence system. Any state of the art intelligence system will have foreign agents attempting to penetrate it in order to gain the upper hand. In the case of the United States, Russia, China, and several Middle Eastern nations are attempting and will continue to attempt to penetrate the intelligence system. Counterintelligence is necessary because the United States must be able to prevent penetration of the intelligence community by these nations in order to defend against espionage and maintain the upper hand. Without counterintelligence, the intelligence community will certainly fall.

References

Bullock, Reginald L. Review of *Espionage: A Reference Handbook*, by Glenn P. Hastedt. *Air And Space Power Journal* 22 (2008): 120. www.proquest.com (accessed November 14, 2013).

Encyclopaedia Britannica Online. S.v. "Counterespionage." http://www.britannica.com (accessed November 13, 2013).

Crane, David M. "Divided We Stand: Counterintelligence Coordination Within the Intelligence Community of the United States." *Department of the Army Pamphlet* 277 (1995): 27-50. www.academic.lexisnexis.com/ (accessed November 14, 2013).

Lowenthal, Mark M. *Intelligence: From Secrets to Policy*. Thousand Oaks, CA: CQ Press, 2012.

Tzu, Sun. *The Art of War*. Translated by Thomas Cleary. Boston: Shambhala Publications, 1988.