ISA Journal of Arts, Humanities and Social Sciences (ISAJAHSS)

Homepage: https://isapublisher.com/isajahss/
Email: office.isapublisher@gmail.com
Volume 2, Issue 2, March-April ISSN: 3049-1827

Counterintelligence: Issues and Challenges

Dr. Peter Sunday Equere[1] and *Capt. Iniobong Edward Ekong*[2]

[1]*Department of History and Diplomatic Studies, Akwa Ibom State University, Nigeria*
[2]*Dept. of History and International Studies, University of Uyo*

Received: 20.03.2025 | **Accepted:** 26.03.2025 | **Published:** 30.04.2025

***Corresponding Author:** *Dr. Peter Sunday Equere*

DOI: *10.5281/zenodo.15322573*

Abstract

Review Article

Counterintelligence is the knowledge needed for the protection and preservation of the military, economic, political, and socio-cultural strength and values of the state, including the security of the government in domestic and foreign affairs against or from espionage, sabotage and all other clandestine activities designed and aimed at the independence, territorial integrity and sovereignty of the state through the infiltration of foreign agents. Counterintelligence is adopted by the intelligence architecture of state as a supportive and complimentary measure of their primary mission of intelligence collection and analysis to ensure the protection of the state secret from espionage by hostile or unfriendly or even friendly foreign powers. The main purpose or essence of counterintelligence is to uncover and thwart foreign intelligence missions against the state. To this end, Specialists of counterintelligence waged a secret war against antagonistic or unfriendly intelligence service and terrorist organisations. This paper is an analysis of the concept, concerns, goals and challenges of counterintelligence. Using the analytical method and relying mostly on secondary sources, the paper argues that the first responsibility of counterintelligence is to protect classified information that are critical to the national security of the state, ensure physical security which involves keeping secret from all except those who need to be aware of it and providing personnel security which involves making sure that the people who are made aware of the state secrets protect those secrets responsibly. The paper in its findings submit that counterintelligence can be seen in three major perspectives – counterintelligence as a product, counterintelligence as an activity and counterintelligence as an organization.

Keywords: Counterintelligence, Intelligence, Espionage, Counter-Espionage, Agent-In-Place, Foreign Intelligence, Secret Agent.

INTRODUCTION:

One of the major concern of States in the contemporary international political system is security threat from foreign intelligence of hostile or unfriendly states since the emergence of modern nation state system. One of the ways adopted by states to address this problem is the use of counterintelligence. Counterintelligence is mostly adopted as a second intelligence mission in support of the primary mission of intelligence. Simply defined, counterintelligence is an activity aimed at protecting the state secrets from espionage of foreign powers. Formally, counterintelligence can be defined as the knowledge needed for the protection and preservation of the military, economic, diplomatic and socio- cultural strength of a state, including the security of its government in domestic and foreign affairs against or from espionage, sabotage and other clandestine operations designed to weaken or threaten the security of the state. [Loch Johnson& James Wirtz,2008:295]. The main goals of counterintelligence is to launch a covert operations against aggressive or antagonistic intelligence services or organizations. This paper is brief analysis of some salient issues of counterintelligence. To this end, the paper is structured in five parts. Part one takes a look at the main concerns of counterintelligence while part two focuses on the nature of counterintelligence as a product, as an activity and as organization. Part three is an analysis on the techniques and functions of counterintelligence and part four addresses the challenges of counterintelligence. Part five is the concluding remarks.

The Concerns of Counterintelligence:

For years, states have been facing various adversaries from the intelligence community and organizations of other states including terrorist groups. For instance, during the cold war era, about 1021 soviet officials were on permanent missions in the United States [George Kalaris & Leonard McCoy,1987:179]. Among them were KGB or GRU – the then Soviet military and civilian intelligence departments, constituting about 40% while the remaining were Soviet diplomats and consular agents. Sometimes, exchange educational programmes provide additional opportunities for intelligence gathering against the national security and interest of state. Sometimes, Foreign students who attend universities in other states are secret agents of their states. For instance, in the 1970s, the United States witnessed an astronomical increase in the number of Soviets immigrants as students to the United States, along with the rise in East- West commercial exchange visitors. [Ray Bearse &Ansthony Read,1991:36]

Also, foreign intelligence agents usually recruit nationals of a state to work for them. There are recruited to disclose classified information regarding the state weapons system as well as commercial activities and strategies. Furthermore, the presence of illegal secret agent in a state poses a serious counterintelligence threats. These illegal agents are people with no easily detectable contacts with their intelligence services. According to the American homeland security organization - Federal Bureau of Intelligence (FBI), these illegals are highly trained specialists in espionage tradecraft. They may be foreign nationals or professional intelligence officers dispatched to various states under false identity. Some illegals may be trained in the scientific or technical fields to permit easy access to sensitive areas of employment. [Mark Riebling,1994:351]

The detection of the presence of these illegal poses a problem to the intelligence community of the host state because once they entered the host state either with fraudulent or true documentation, their presence is obscured among the thousands of legitimates immigrants. Relatively un-detected, they are able to maintain contact with their foreign masters by means of secret writings, microdots and open signals in conventional communication gadgets that are not susceptible to discovery through conventional investigative measures. [Roland Kessler,1989:30].

The espionage activities of states or clandestine operations of terrorist organisations against the territorial integrity of states as well as their citizens, troops, diplomats and interest abroad possess a serious security threat and are extensive and relentless especially from enemy states or insurgent or terrorist groups. To counter or contain these threats, a state counterintelligence department must develop superlative investigative techniques to obtain information about the activities of the enemy state or adversaries at home and abroad and to protect its intelligence operations and community [Roland Kessler,1989:31].

Nature of Counterintelligence:

This part of the paper examines the nature of counterintelligence to include counterintelligence as a product, as an activity and as organization.

[a] Counterintelligence As a Product: Counterintelligence is as a product has to do with information about the enemy of the state. This product is reliable information about all unfriendly or hostile foreign intelligence services and other threats such as the activities of terrorist cells within the state. Counterintelligence as a product make it necessary to understand the organizational structures of the enemy, its key personnel, its method of recruitment and training and the details of specific operations. The efforts of intelligence services in the international community to conceal such information from one another through security devices and elaborate deceptions creates what James Arlington, one time Central Intelligence Agency [CIA] Chief , called “wilderness of mirror”, a term he borrowed from the poet, T. S. Eliot. [Frank Greve,1992:87].

[b] Counterintelligence as an Activity: As an activity, counterintelligence involves two matching halves – counter espionage and security. Counterespionage consists of the offensive or aggressive side of counterintelligence. It involves identifying specific adversaries and developing detailed knowledge about the missions or operations they are planning or conducting. Counterespionage agents attempt to thwarts these missions by infiltrating the rank and file of the enemy service, an operation known as ‘penetration’ amongst intelligence operatives. They also uses sundry forms of manipulations to achieve their set goals or targets. Practically, the thrust of the hostile operations is turned against the enemy.

In the area of security, counterintelligence is the passive or defensive side of intelligence. It entails putting in place defenses against all hostile and covert operations at the state, regardless of who is behind such operations. These security defenses include screening and clearance of personnel and establishment of programmme, to safeguard sensitive intelligence information- what is known as the administration of security control. The essence of these measures is to defend the personnel, installations and operations against enemy intelligence services and terrorists. The specific defensive measures used for information control by counterintelligence agents include security clearance [consisting of thorough inquiries into the background of jobs candidates] polygraph, locking containers, security education document accountability, censorship, camouflage and codes. [Peter Schweitzer,1998:139].

Beyond these, devices for physical security include fences,, lighting system, alarms, badges and passes. The control of a specific area relies on curfew, check points and restricted zones. The security side of counterintelligence concerns perimeter defence, badges, full knowledge of the foreign intelligence services, while the counterespionage involves knowing all about foreign intelligence services, - their people, installations, methods, and their operatives. [Ruth Sanai, 1993: 90].

[c] Counterintelligence as Organization: It is part of the responsibilities of the security aspect of counterintelligence to protect the personnel and installations while the counterespionage operations are mainly to take on the foreign services of the enemy state. Also, to combat terrorism, effectively, more units are created depending on the status and national power of the state to undertake covert operations. For instance, the terrorist bombing of the world trade center in New York in 1993, the bombing of the federal building in Oklahoma city in 1995 as well as the bombing of the American embassies in Kenya and Tanzania in 1998 prompted the American congress to fund expansively the counterintelligence units charged with combating terrorism to contain these attack on American interest abroad. After the September 2001 terrorist attack, the American government increased its funding on counterintelligence. [Johnson & Wirtz, 2008:297]

Techniques of Counterintelligence:

There are many types of operations in counterintelligence. These variants make up the techniques of the missions. Here the paper considers few cases to bring to the fore the various techniques of counterintelligence. These include the penetration and the double agent, the defector, the deception operation, counterintelligence and research and counterintelligence and liason.

[a] **The Penetration and the Double Agent** : Many techniques of counterintelligence exist but the most important is the penetration or what is known within the intelligence community as the 'mole'. Bearing in mind that the primary goal of counterintelligence is to contain the intelligence service and saboteurs of the enemy state, it is necessary to know their detailed plans in advance. One of the ways to achieve this is through infiltration of the of the enemy's intelligence or government. This position is underscored by the words of John Macone, one time director of the CIA, in charge of counterintelligence when he said "Experience has shown penetration to be the most effective response to Soviet and bloc intelligence service" [Johnson & Writz, 2008:298]

In addition, a strategically placed infiltrator in a hostile intelligence is preferable to any option in determining whether one's own service has been penetrated by an outsider. Experts in intelligence studies have affirmed that there are three basic ways good enough to meet, neutralize and defeat hostile penetration. These are security screening, clearance of personnel and effort to physically safeguard sensitive intelligence information. Methods of infiltrating the opposition service takes various forms. One of the most effective ways is the recruitment of agents- in- place. Such agent is already in the employ of an enemy intelligence service. Various inducement may be used to entice the recruit. Money is the most effective and popular bait.

If recruitment is successful, an agent- in- place can be very useful since he is presumably already trusted within his organization and will have unquestioned and unhindered access to key secret or classified document. Another method of infiltration is the double agent. However, double agents are expensive, time- consuming and risky because the loyalty of the agent is very questionable with double crosses being the name of the game. The running of double agent entails much pure drudgery with few remarkable results as new information must be constantly and painstakingly checked against existing files or records. Also, passing credible information back to the enemy to ensure the credibility of the double agent can be an uphill endeavor. The operations must appear plausible to the enemy to make fake papers seems realistic while the genuine papers must be provided repeatedly. In this process, classified information must be cleared since it is the tradition in intelligence service to release any classified document to outsider reluctantly. This means allowing a lot of good intelligence to get to the enemy without much in return. To achieve these targets requires hard work, careful planning and considerable staff resource. [Yuri Shvets,1994:35].

[b] The Defector : The defector with knowledge is as good as the agent -in – place and with less problem to manage than the double agent. In this case, the challenge is how to thoroughly interrogates and validates the defector to fit into your mission, by providing the agent with a credible mix of false and genuine documents along with other logistical support. Although an agent – in – place is preferable because he or she already has useful intelligence he or she can give, but the agent – in – place does not want to take the risk of staying in – place, especially where there is sophisticated security network and where the traitor pays the supreme price if caught. The agent prefers to defect to safety in a another but safer clime. Consequently, the agents – in – place are difficult to come by in a tightly controlled regimes with robust counterintelligence service of its own. This tight situation always facilitates defection. On the other hand, the agent – in – place are easily recruited in developing states where security network is poor, thereby creating the enabling environment for them to operates with ease. [Ruth Sanai, 1993:124.]

In the case of the United States, defectors recruited abroad by the Central Intelligence Agency, [CIA] are occasionally brought to the country to resettle, especially if such defector is very important and likely to provide useful information or someone who had already provided such information and now seek exfiltration to avoid arrest and execution in his or her country. In such cases, the Federal Bureau of Investigation, [FBI] is notified, and after the CIA had completed its investigation, the FBI counterintelligence operatives may interrogate. Terrorists captured in the United States are normally interrogated first by officers of the FBI, then by the CIA, but the process is vice versa in the case of terrorists captured abroad [Lynn Fischer, 2001: 13]

[c] The Deception Operation: The penetration [mole] and the double agent are closely related to deception operation which is another technique of counterintelligence. The deception operation is an attempt to give to an enemy a false impression about something causing him or her to take action contrary to his or her interests. One classical example of deception operation occurred during the second world war when the Germans were fooled into believing that the D- Day landings would be at the Pas – de-Calais rather than in Normandy was a classic example of a successful deception operation during the II world war.

Deception is related to penetration because the state's agent – in – place operating within foreign intelligence agencies can serve as a veritable channel through which misleading information can flow to an enemy. Therefore, mole and double agents can serve as collectors of intelligence and instruments of deception. Sometimes, a state intelligence service can allow foreign penetration into its own intelligence service, and then carefully feed fake information to its enemy through him. This is another approach of deception operation. [David Wise,1998:294]

[d] Other Methods of Counterintelligence : Other techniques of counterintelligence include surreptitious surveillance of various types including audio, mail, physical and optical surveillance, as well as interrogation, sometimes keeping the subject incommunicado until his or her true mission is known. Part of these methods include decoding of secret messages sent by an enemy to a mole, trailing suspected agents. Observing 'dead drops' [exchange of materials such as secret documents or instructions between a spy and his handler], and photographing individuals entering opposition embassies or other government establishment. Since the main aim of offensive counterintelligence is to disrupt the enemy intelligence service, provocation can be an important element of counterintelligence. This approach involves harassment of an enemy such as publishing the names of his agent or sending a trouble- making false defector into its midst who in reality, an agent provocateur. [Johnson &Writz,2008:299]

The Functions and Techniques of Counterintelligence : Counterintelligence serves many functions using various techniques. This part of the paper discusses in details these functions and techniques.

[1] Protecting the State Secrets : The first very important function of counterintelligence is to protect state information that are classified and hereafter referred to as secrets and are critical to the national security of the state. This function entails two aspects – physical security which involves keeping secrets away from all except those who need to be aware of them and personnel security which involves ensuring that the people who are made aware of the state secrets protect those secrets responsibly. Other security measures include ethnic recruiting, technical security issues and encryption. Details of these measures are discussed below.

[a] Physical Security : Much of physical security involves mechanical measures – safes, password, identification badges, security guards, alarm and other related measures. However, the latest of these measures is to sale this measure to foreigners. Thus, giving the opportunity to study these system and later device counter measures. The most obvious of physical security are the keeping of potential foreign spies away from classified information, by denying them access and preventing them from interacting with people. Exit control – preventing spies from walking off with classified document. Securing films and disc is another measure of physical security. adopted by Counterintellingence operatives [Bob Drogin, 1999 :65]

[b] Foreign Employees: Foreign employees can be the target by their home intelligence services if they occupy positions with access to secrets. This is so because hiring of foreign nationals by a state poses security challenges. For instance, French intelligence services always place its employees within targeted U.S. firms with high tech secrets while Chinese counterintelligence regularly uses its scientists in U.S firms as intelligence sources and collectors. [Nicholas Ehimiades,1994:121] Also, for decades, American counterintelligence pleaded with U.S. State Department diplomats to reduce or do away with granting access to local employees at the U.S. embassies and consulates, especially employees from Eastern and Central Europe. It was a common knowledge within the intelligence community that local employees from these Warsaw Pact states were spies for the KGB.

The cases of construction and renovation of offices abroad has its security problems. A typical case was the case of the U.S. embassy in Moscow. In 1953, the U.S. embassy in Moscow moved to an apartment which was reconstructed using local employees. In 1946, it was discovered that forty -seven microphones were built into the walls of the apartment as well as a secret tunnel leading out of the basement. Also, in 1979, in constructing the U.S. embassy chancery building in Moscow, the State Department allowed Russian nationals to supply building materials. After construction, it was discovered that the building was riddled with hundreds of listening devices. [Ronald Kessler, 1989:231]

[c] Visitors : At the end od the cold war, states like the United States, relaxed its physical security safeguards at installations housing state secrets. Before that, in 1985, the director of the CIA raised concerns about the foreign visitors to the U.S. Department of Energy. The access by foreign visitors to places like these buildings and installations exposed the American classified document to enemy states Consequently, the 1999, President's Foreign Intelligence Advisory Board special report cited many cases of sloppy and non- existent safeguarding of classified documents at the Department of Energy nuclear laboratories The report also had a case of missing of a top secret intelligence file from Madeline Albright, the then Secretary of State's office, linked to unidentified man. According to information in the 1999 U.S. Defense Authorization bill, 6,398 visitors visited the three weapons labs. owned by the Department of Energy [DOE] where nuclear and other weapons research and development is conducted and weapons information are stored. Of this number,1,824 where from states like China, Russia and India. [Mark Riebling,1997:314]

[d] Exit Control : It is true that other government agencies or bodies may be negligent concerning physical security. Fawn Hall, the confidential secretary of Oliver North, a director at the National Security Council during the administration of President Ronald Reagan of the United States, confessed to the U.S congress that she removed secrets and very classified documents from the White House by concealing them in her clothing, Jonathan Pollard regularly walked out of the U.S Naval Intelligence Center with his briefcase full of secret papers meant for the Israelis, among others.] Norman Polmar, 1997:43] These cases demonstrated what other countries are suffering due to acts of negligence and is indicative of government in general. Also, the elementary precautions of keeping intelligence operatives away from facilities and personnels who are with state secrets is used means of exit control.

[e] Personnel Security : The logic behind personnel security is to ensure that those who have access to state secrets because of their jobs are people of proven integrity and probity, who will not disclose these secrets. This assumption is not always the case, resulting in creating more problems for counterintelligence. Key elements of personnel security counterintelligence are background investigation, re-investigation, polygraph examination and 'the need to know' notion. Other measures include the detection of employees with alcohol and narcotic substance abuse, financial and marital problems that might affect their performance as custodians of state secrets. [Vernon Loeb,1999:26]

[f] Background Investigations: A major step in the personnel security process is the background investigation. This is done when someone is proposed for a security clearance which gives access to state secrets. It is on record that this counterintelligence measure has not been properly utilized, thereby allowing people who ordinarily are not loyal or supportive of the government of the day to occupied sensitive positions in government. However, people who handles these background investigations are not adequately rewarded and the job has no career prospects. Also, civil liberty organizations are fond of preventing investigators from access to employees' bank details and investments as well as lifestyles. Consequently, background investigations tend to be cursory, involving interviews of he references, the application listed as well as verification of employment, academic records and checking the person's name with law enforcement agencies for criminal records. [David Wise,1988:98]

[g] Re- investigation : Only very few intelligence bodies regularly conducts re-investigation of employees after some years in service. Here an employee that acquires a top- secrets or special access to classified information, should be subjected to re-investigation at least every five years. However, experience has shown that the re-investigation is always mere review of employee/s files without any new investigations. This makes re-investigation unserious counterintelligence check. [Walter Pincus, 1999:121].

[h] Polygraph examinations: Polygraph examinations plays three counterintelligence functions. One, they intimidate potential disclosers of state secrets from doing so for fear of being caught. Two, when used on regular basis they can detect deceptions which can result in self- confession or more routine but intensive scrutiny and three, they can be used as follow up investigative tool should a person come under suspicion from other mean. The polygraph examination is a very vital and reliable tool of counterintelligence [David Wise,1988:36]

[2] Frustrating Foreign Intelligence Operatives : The second functions of counterintelligence is to frustrate the efforts of foreign intelligence operatives to steal the state secrets. This can be achieved using various methods such as expelling them, denying them access or entry, controlling their movement and access, surveilling them through physical or electronic means and using 'double agents' to preoccupy or misled them. For these methods to work well, one precondition is very necessary - knowing who the operatives are.

[a] Identifying the Operatives : One important aspects of any counter intelligence is having an accurate knowledge and sharing of information among the intelligence agencies. This aspects of counter intelligence has gone through many reforms in-order to have an idea of the known and suspected foreign intelligence operatives and their mode of operations. Record keeping is very essential in any counter intelligence programme, which must be built up mostly from painstaking debriefing of intelligence defectors and assets as well as examinations of the results of double agents cases and the surveillance of intelligence officers. During the cold war, there was widespread sharing among NATO allies of information on Warsaw Pact intelligence personnel, identification and record keeping. [John Grey, 1999:89]

[b] Expelling or denying entry to intelligence officers : One of the effective ways a state can use to suppress foreign spying is the expulsion or denial of entry to intelligence officers, even though it is a short term measure. This is so because most of the intelligence cops operates courtesy of the diplomatic cover and protection of their foreign missions. Even when some of them came as accredited diplomats, their visas are subjected to extra and rigorous scrutiny by counterintelligence service. During the cold war, counterintelligence operatives from NATO countries exchanged intelligence on hostile intelligence officers and denying visa to known or suspected intelligence operatives effectively contained the offensive intelligence of enemy states, especially from the WARSAW Pact allies..

Another method of containing the operations of foreign intelligence service is the expulsion of these officers. For instance, in 1971, the British government frustrated the operations of the KGB, the intelligence personnel of the then Soviet Union, when the then Prime Minister, Edward Heath authorized the expulsionof105 KGB officials. In 1986, the then President of the United States, Ronald Reagan authorized the FBI, a branch of the American intelligence community to expel 80 KGB officials that operated under the diplomatic cover from the United States. Christopher Andrew, a KGB defector, confirmed that the 1971 expulsion brought the golden age of KGB operations to an end because the British residency were never recovered. However, Paul Redmond, a retired CIA director maintained that despite these expulsions, the Russians intelligence in the United States as at 2008 were larger than what it was at the apogee of the cold war. In practical terms, despite the effectiveness of expulsions with publicity and visa denials of foreign intelligence, states rarely adopt these measures because the foreign government will always retaliate even though it may not be proportionately and it does not promote friendly relations between the two states. Also, very vital bilateral or multilateral agreements or even trade relations may be jeopardized as the results of these expulsions. It also creates room for mutual hostilities and diplomatic row. This is why in most cases political leaders don't always encourage it but go for it in extreme cases. [Grey, 1999:91]

[c] Use of physical surveillance : Physical surveillance is one of the commonest techniques of counterintelligence services, though it is labour intensive and boring, with little positive results. These methods are in three folds – static surveillance, mobile surveillance and electronic surveillance. Static surveillance has to do with the physical observation of a place, suspected residence, apartment or what is called a "choke point" in intelligence community, where suspects are usually found. It can even be the chancery of a diplomatic mission whose personnel include intelligence operatives. This method of surveillance serves three purposes – to alert a mobile surveillance team when a suspect exit or passes by so that the team can arrest such suspect, take note of the movement of suspects or visitors and identify would be spies in a foreign embassy to volunteer their services. These measures count much in counterintelligence and informed the presence of surveillance units in foreign missions. All said, static surveillance contributes very little to counterintelligence [Bob Drogin,1999:126]

[d] Mobile Surveillance: This technique of counterintelligence can be done in many ways such as on foot, motorcycle, vehicle and aircraft. This type of surveillance is very common the world over and extremely labour intensive but prevalent in the states of the global south where there is cheap manpower. It is designed for two purposes - to intimidate and discourage a suspect from undertaking an illegal act relating to espionage and arresting the suspect in the act of undertaking such act of espionage. This measure is always combined with fixed point or electronic surveillance.

[e]Electronic and other Means of Surveillance: Electronic surveillance through telephone taps, electronic listening devices [bug] and other means of surveillance are used to frustrate foreign intelligence by identifying their contacts, blocking their communications and converting them possibly into double agents. Electronic devices also play a vital role in mobile surveillance by using beacons which detect the exact location of vehicle or person. These special electronic surveillance devices play vital roles in successful counterintelligence as teltaps and bugs are used for establishing contact, tracking of movement of suspects and other purposes. These devices serve as primary tools of collecting of evidence of espionage once a suspect is identified as a spy or a foreign diplomat who serve as an intelligence operative. They can also be used to gather evidences about the character of an intelligence operatives. The use of electronic surveillance in dealing with the problem of espionage is limited in practice, meaning that counterintelligence operatives need to go beyond the use of electronic surveillance in the discharge of their covert operations.[Lynn Fischer,2001:15]

Challenges of Counterintelligence:

There are many challenges to counterintelligence. Some of these challenges borders on the domestic laws of the state, bureaucratic bottlenecks and cultural values and norms of the society. The paper examines these issues in the remaining analysis in this part.

The laws on espionage embedded in the municipal regime of a state can pose serious challenges to counterintelligence. There are laws which demand that four criminal elements must be proven before an espionage conviction can be sustained. These include: the accused person must be knowingly communicate or deliver the state secrets or classified document to a foreign entity or state, such materials must have serious bearings to the national security of the state and it must be established that such act was carried out intentionally to injure or affect adversely the interest of the state or to the advantage of a foreign state or entity. Considering the nature and operations of espionage, meeting these conditions can be cumbersome before a criminal case is established and sustained on a suspected spy except where the suspect is caught in the act or he or she confess of the act. Even when these four elements appears to have been established, another hindrance is the so- called right of 'discovery', a law which, on the demand of the suspect in court, compels an intelligence agency to tender its classified document for examination. For instance in 1948, Judith Coplon, an American intelligence operative was caught giving out very classified documents to her lover, a Russian KGB intelligence official. During the trial, her lawyer demanded, under the right of discovery for all FBI files remotely related to the case. Though the judge reluctantly obliged, the consequences of divulging state secret undermind to very large extent the national security of the United States. The fear of exposing state classified document, though may not be applicable in all judicial system, may not encourage trail of suspects caught in the act of espionage. However, in 1980, the American congress addressed this matter by passing the Classified Information Procedure Act which allows the government to present the demanded classified document in camera to the trial judge. [James Rowley,1993 :143]

Another challenge to counterintelligence is the nature of political and societal values and norms. Alexis Tocqueville, in his seminar work, 'Democracy In America' argued that democracies are not good at secrecy. [James Rowley,1993: 150] Practically, most democratic societies don't like nor encourage secrecy. Here, classified information of state are sometimes found on the pages of newspapers. Another issue has to do with dislike of informers or whistle blowers. In some societies, for one to tattle [tell secret about what someone else has done] on others is a very serious violation of societal norm. In these societies, defectors are not well received nor informants are treated with respect. People always declined to report on others on the ground of minding their business. Distrust of government and security agencies is another serious challenge to counterintelligence. [James Rowley,1993:153]. it is common knowledge that in most cases, people that gives information to security agencies are exposed to danger or threat because of poor management of the information on the part of the security operatives. For instance, most Nigerians refuses to give intelligence to the Nigeria Police and other security agencies for fear of exposure and possible danger to their lives. Historically, African societies are communal societies where what affects one affect all in local community settings. Africans before today were always interested in what goes on in their community and neighbourhood. Parenting and guardianship of children were collective responsibilities of the adults, regardless of filial relationship. Visitors or strange persons were accepted but with caution and the desire to know his origin, mission and intentions. In some communities, a family that has a visitor or guest must introduce such guests to neighbours and leaders of the community. This communal nature of African society suits the goals of counterintelligence, but today western culture and values have eroded this African values and norms.

Another challenge to counterintelligence is bureaucratic bottlenecks. Expert of organizational behaivior affirm that bureaucracies don't operates smoothly without unnecessary hitches. The common bureaucratic response to a short fall in government is to ask for more money and create more bureaucratic bodies to address intelligence problems.

Concluding Remarks:

This paper has examined issues on counterintelligence. It discussed counterintelligence as a product, as an activity and as organization. The penetration of a double agent, the defector, deception operation and other counterintelligence methods have been highlighted as major techniques of counterintelligence. Furthermore, the paper has analysed the various functions of counterintelligence to include the protection of state secrets by providing physical security, monitoring of foreign employees and visitors, personnel security, conducting background investigations and re-investigations, frustrating foreign intelligence operatives by knowing who they are, taking records of their movement and activities, expelling and denying entry to foreign intelligence operatives and providing physical surveillance. Finally, the paper interrogated reasons that militates against smooth and hitch-free counterintelligence.

REFERENCES

Bob Drogin*, " Secrets Science Are Volatile Mixture at Los Alamos",* in Intelligence, New York : Praeger,1999.

David Wise, *The Spy Who Got Away*, New York: Random House,1988.

Frank Greeve *" In the World of Espionage, France emerges as U.S. Adversary*" Philadelphia Inquirer, 1992.

George Kalaris and Leonard Mc-Coy, *Counterintelligence for the 1990s",* International Journal of Intelligence and Counterintelligence, Summer,1987.

James Rowley, *"FBI Seeking Scores of Once KGB Spies Book Says"* Washington D.C. Associated Press, 1998.

John Grey*, "Gaffes Damages Intelligence Agency's Image",* South China Morning Post, December 1999.

Loch Johnson & James Wirtz, Intelligence and National Security, 2nd ed. New York: Oxford University, 2008.

Lynn Fischer*, " Espionage: Why Does It Happen",* Security Awareness Bulletin, Department of Defence and Security, Boston, 1998.

Mark Riebling, *The Secret War Between The FBI and CIA*, New York : Alfred & Knoff, 1994.

Nicholas Ehimiades, *Chinese Intelligence Operations*, Maryland : Naval Institute Press, 1994.

Norman Polmar & Thomas Allen, *Spy Book*, The Encyclopadia of Espionage, New York :Random House,1997.

Peter Schweitzer*, Friendly Spies : How America's Allies Are Using Economic Espionage To Steal Our Secrets*, New York: 1994.

Ray Bearse & Anthony Read, *The Untold Story Of Tyler Kent*, New York : 1991.

Ronald Kessler, Moscow Station*: How KGB Penetrated The American Embassy*, New York: Pocket Books, 1989.

Ruth Sanai, *"Its Not So Hard To Walk Out With Secret Documents."* Associated Press, 1993.

Vernon Leob, *" Senators Challenge Energy Polygraph Plan",* Washington Post,1999.

Walter Pincus, *"Huge Backlog For Security Check Tied To Pentagon Computer Woes,"* Washington Post, 1999.

Yuri Shvets, Washington Station: *My Life As A KGB Spy in America*, New York : Simon & Schuster, 1994.