

This document is made available through the declassification efforts
and research of John Greenewald, Jr., creator of:

The Black Vault



The Black Vault is the largest online Freedom of Information Act (FOIA)
document clearinghouse in the world. The research efforts here are
responsible for the declassification of hundreds of thousands of pages
released by the U.S. Government & Military.

Discover the Truth at: <http://www.theblackvault.com>



DEPARTMENT OF THE NAVY

U.S. NAVAL WAR COLLEGE
686 CUSHING RD
NEWPORT RHODE ISLAND 02841-1207

5720
Ser N002/0268
May 2, 2018

John Greenewald, Jr.
27305 W. Live Oak Rd, Suite 1203
Castaic, CA 91384

Dear Mr. Greenewald:

This letter is in response to your request under the Freedom of Information Act (FOIA) request, in which you seek the document "Counterintelligence/counterespionage in the U.S. Navy," AD Number: ADB148757, dated May 14, 1990, and assigned Case File Number NAVWARCOL 2018002.

The document is provided with redactions, pursuant to exemption (b)(6) of the Freedom of Information Act, 5 USC § 552, which protects personal information. No fees were associated with the processing of your request by this command.

You have the right to an appeal. It must be received within 90 calendar days from the date of this letter. Please provide a letter requesting an appeal, with a copy of your initial request and a copy of the letter of denial, in an envelope marked "Freedom of Information Act Appeal." You are encouraged (though not required) to provide an explanation why you believe the redactions were inappropriate or our search was inadequate.

To ensure that your request is received by the deadline, I recommend that you make your appeal by using FOIAonline. To do so, go to FOIAonline (a website which appears as the top item if you search the internet for "FOIAonline"), establish an account if you have not already (click "Create an Account," the bottom of three green buttons on the right of the FOIAonline home page), locate your original request (enter a keyword or the tracking number of the request in the "Search for" field on the "Search" tab), click on the request, and then click on the "Create Appeal" tab in the left-hand column. The basic information from your request will be duplicated for you, and you can type in the basis of your appeal.

Alternatively, you may mail your appeal to:

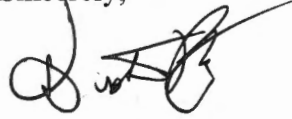
The Judge Advocate General (Code 14)
1322 Patterson Avenue SE, Suite 3000
Washington Navy Yard, DC 20374-5066

Please also mail a copy of the appeal to us at:

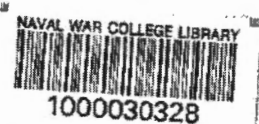
U.S. Naval War College
President - 005
686 Cushing Rd,
Newport, RI 02841.

If you have any questions, please contact the U.S. Naval War College FOIA Coordinator by telephone (401)841-2279 and cite the case number provided above. You may also contact the DON FOIA Public Liaison, Christopher Julka, at christopher.a.julka@navy.mil, (703)697-0031.

Sincerely,

A handwritten signature in black ink, appearing to be 'J. D. Pilling', written over a horizontal line.

J. D. PILLING
CDR, JAGC, USN
By direction



#138

NAVAL WAR COLLEGE
Newport, R.I.

COUNTERINTELLIGENCE/COUNTERESPIONAGE
IN THE U.S. NAVY

by

(b) (6)

GM14 - NIS



A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature:

(b) (6)

14 May 1990

Paper directed by COL (b) (6) (b) (6)
Chairman, Department of Operations

Approved by:

Faculty Research Advisor Date



TABLE OF CONTENTS

CHAPTER	PAGE
ABSTRACT	ii
I INTRODUCTION	1
II THE THREAT	3
III THE TARGET	8
IV DOD SECURITY RESPONSIBILITIES	12
V NIS COUNTERINTELLIGENCE	15
Double Agent Operations	16
NIS Espionage Investigations	17
Passive Listening Post Program	17
PACE Program	17
Preventive Counterintelligence	18
VI REVIEW OF RECENT NAVY SPIES	19
VII FUTURE COURSES OF ACTION	23
VIII CONCLUSIONS	27
APPENDIX A--ORGANIZATION OF THE KGB	29
B--ORGANIZATION OF THE GRU	30
C--DOD FOREIGN COUNTERINTELLIGENCE	31
D--NIS COUNTERINTELLIGENCE DEPARTMENT	32
NOTES	33
BIBLIOGRAPHY	35

ABSTRACT OF
COUNTERINTELLIGENCE/COUNTERESPIONAGE
IN THE U.S. NAVY

The Soviet Union, its surrogates and other countries hostile to the United States, identify the U.S. Navy as a primary target for espionage. They want the Navy's classified information and critical technology. The Naval Investigative Service (NIS) has the primary mission of combatting espionage and protecting the Department of the Navy from the efforts of hostile intelligence services. This paper focuses on our primary espionage threat, the Soviet Union, and describes its tactics and targets. The current NIS counterintelligence effort is examined and some of the recent Navy spy cases are reviewed. The paper concludes with recommendations for future courses of action to better protect the Navy from espionage.

I. INTRODUCTION

What makes a spy? Who are they? Have you ever wondered how spies are caught? Why have so many surfaced in the U.S. Navy and Marine Corps? One of the primary missions of the U.S. Naval Investigative Service (NIS) is counterintelligence (keeping hostile nations from stealing our secrets) and counterespionage (identifying and neutralizing spies against the United States). Are there more spies in this unique venue or are we just doing a better job of catching them? Determining whether there are more or not does not solve the problem. The damage spies can do to our national security is enormous. One only has to look at the so called "Walker Spy Ring" where more than 17 years of active espionage was performed on behalf of the Soviet KGB to understand the damage that can be inflicted.¹ This paper will examine the overall threat from hostile nations seeking our military secrets, describe the individuals the Soviet Union and other hostile nations target, review the Department of Defense security responsibilities, examine the NIS strategy and current operations to deal with the threat, and recommend future courses of action to combat espionage and increase the Department of the Navy's security posture.

The 1980's may well be remembered as the decade of the spy. As a nation we cannot afford a repeat in the 1990's. Our well-earned freedom depends on maintaining a qualitative edge over the Soviet Union. We cannot be lulled into complacency because of the break-up of the Warsaw bloc countries. Nor can we believe that

Gorbachev's program of perestroika, which portends to set the "revolutionary" goals of "rebuilding" the economy, "restructuring" the existing Soviet socio-political system, and introducing "new thinking" into their relations with the west, will decrease their military capabilities.² Cuts in Soviet military spending are being made. However, there have been no indications that reduction will be occurring in modernization of technological advancements. "Successful espionage and technology transfer will contribute to Gorbachev's goal of reducing his military budget while improving his security posture vis-a-vis the west. Soviet espionage is potentially the most lethal threat to U.S. military capabilities today."³

Deterrence of war has been the cornerstone of American policy for over forty years. The U.S. Navy's maritime strategy is a principal contributor to the deterrence equation. The strategic submarine force, forward deployed carrier battle groups, Navy and Marine amphibious task forces, all provide the range of options which serve to bolster deterrence through credibility. We cannot allow hostile intelligence services to compromise Naval assets, especially our personnel.

II. THE THREAT

Each year thousands of programs and projects and millions of documents are classified by the Department of Defense (DOD) through its components in a wide area of operational and geographical settings. They are classified because of national security implications. The intelligence services of the Soviet Union, its surrogates and other countries with interests hostile to the United States want to obtain our secrets to increase their knowledge, capabilities and resources, while learning our capabilities.

Protecting the nation's secrets is an age-old challenge. However, we are also the most open and free society the world has ever known, and most of our people would have it no other way. We are indeed a ripe target. But because of the extraordinary importance of advanced technology to our nation's military capabilities, its loss to a potential adversary by espionage, theft or other unauthorized disclosure, can be crucial to the military balance. Thus our ability to safeguard classified information from those who would oppose us is critical. To do this in our open society presents real difficulties.

Our primary adversary is of course the Soviet Union and within the Soviet Union, the KGB and the GRU. The KGB gets its name from the Russian words Komitet Gosudarstvennoy Bezopasnosti, which translates as the Committee for State Security.⁴ It is an incredibly large organization that concerns itself with all aspects of

Soviet life. Espionage is but a small part of the activities of the KGB. Still, the KGB's Chief Directorate is the largest intelligence service in the world.⁵

What are the goals of the Soviet Union and the KGB? This is a tough question in these days of perestroika and glasnost, however, (b)(6), a former KGB agent and defector answered the question in 1988 this way:

"...Since the 1950's the Soviet leaders have considered the United States their No. 1 enemy, and the main thrust of the KGB's activity on a global basis is directed against the United States. I know this is true because that goal was exactly what I was committed to serving for so long, especially during the turbulent four years and eight months I served as a political intelligence and active measures officer in Japan.

I often hear people say that Mr. Gorbachev is a "new Russian", that his new image indicates a new approach in Soviet politics. Mr. Gorbachev, regardless of the reforms he promises in industry and agriculture, does not intend to change the main goal of socialism, clearly defined by Marx, Engels, Lenin, and Stalin. According to their theory, which all Soviet leaders, including Mr. Gorbachev, have been and are implementing in practice, the socialist system should prevail over capitalism--everywhere."⁶

While not as large or as strong as the KGB, there is also the GRU (Glavnoye Razvedy-Vatelnoye Upravleniye) or Chief of Intelligence Directorate of the General Staff. The GRU makes up the military intelligence collection effort of the USSR.⁷ Since these two agencies are considered to be the primary hostile "Human Intelligence" (HUMINT) threat to the Department of the Navy, they are the focus of concern for this paper. However, while the

Soviet Union is the focus of our concern, U.S. counterintelligence agencies must be concerned with a myriad of additional threats. The Peoples Republic of China concentrates primarily on advanced technology for military and economic modernization rather than U.S. and NATO plans, intentions and capabilities. Countries such as North Korea and Nicaragua pose a lesser, but still significant threat because of their presence in the United States and in our spheres of influence and interests. Interestingly, a number of allied, friendly and neutral countries engage in intelligence operations against the U.S. (lest we get too smug, we do the same to them). The case of Jonathan Pollard demonstrated the critical, embarrassing, poignant fact that Israel had been collecting against the United States for a number of years. Pollard's case will be examined in further detail in the "Review of Recent Cases" section of this paper.

The KGB functions include intelligence collection, domestic and foreign counterintelligence, covert operations, executive protection of the Soviet leadership and border security. Special forces units (SPETNAZ) are also integrated into the KGB. It is estimated the KGB has "between 500,000 and 750,000 employees, including 40,000 headquarters personnel, 100,000 domestic informants, and 30,000 to 50,000 communications troops".^B It is interesting to note that the Soviet people appear to fear the KGB more than we do. (b) (6) in his book Breaking with Moscow discusses this fear. (b) (6) was

a Soviet diplomat assigned to the United Nations when he defected to the United States.⁹

The element of the KGB that conducts foreign espionage, the First Directorate, has an intelligence mission similar to, but much broader than, our Central Intelligence Agency. Its various departments control intelligence officers operations under diplomatic or commercial cover as well as illegal agents, assassination and sabotage planning, political, scientific, industrial and technical collection operations. The First Department of the First Directorate is responsible for operations in the U.S. and Canada. Appendix (A) details the structure of the KGB.

The Chief Intelligence Directorate of the Soviet General Staff (GRU) is yet another formidable intelligence agency. The primary function of the GRU is the collection and analysis of military and related intelligence for the Soviet armed forces, but its collection efforts involve far more than military information. The GRU frequently is involved in the theft and illegal transfer of technology from the west. The Second Directorate of the GRU--North American Affairs--conducts intelligence operations within the United States. Appendix (B) depicts the GRU organization.

While the Soviet Union controls a very capable technical collection network, its intelligence services are deeply committed to human intelligence operations. "Soviet HUMINT Operations normally involve a KGB or GRU line officer, under official or non-official cover, who recruits and controls an individual agent or network of

agents to clandestinely obtain specific items of
information not legally available to the Soviet Union."¹⁰

III. THE TARGET

Agents for the Hostile Intelligence Service are normally not professional intelligence officers but rather citizens of the target country (or if you will, spies). Citizens employed by the government, military and the military industrial complex are the most likely targets. The reasons are obvious, this is where our secrets are held. This is where our national security lies. Recruitment may occur through friendship, ideology, coercion, blackmail or the favorite of the current breed, monetary gain.

In the wake of recent American spy trials, it seems clear that Americans become spies for the money. Yet Americans seem very patriotic and have one of the highest standards of living in the world. How can we explain the Jerry Whitworths and John Walkers of the world? The former KGB agent (b)(6) has some ideas:

"First, the United States is the prime consumer country in the world. People in this country are brought up on television, and one of the things that television does well is saturate generation after generation with attractive pictures of the good life and the promise that this good life will be better if such and such product is added to it. Children seem to grow up expecting that they will be able to buy what they want when they want it. Unfortunately, there are many people who will not reach such heights in income and purchasing power. When that is compounded by the easy availability of credit cards and the promise of buy now pay later, the risk of finding oneself in debt certainly exists. It is possible that some who sell out to the enemy are people who have entrapped

themselves by assuming that they have a right to more and more consumer goods and unwisely have gone too deeply in debt."¹¹

Not only do the Soviets target individuals who have access to classified information and have financial trouble, but these individuals also seek out foreign countries that are willing to buy our secrets. The question needs to be asked, if these individuals thought they would be caught would they risk turning traitor? Unfortunately, it appears that most do not think the risks are very great. One must also take pause and reflect upon the possibility that most spies are not caught.

Soviet officers under official cover are identified as "legals", since they are legally in the country and operate from an embassy, consulate, trade mission, or some other official Soviet installation. A "legal" also enjoys in most cases diplomatic immunity if arrested for espionage. Soviet representatives engaged in espionage activity and who do not have diplomatic cover, normally work within the Soviet News Agency Tass, Amtorg Commercial Trading Company, Intourist and Aeroflot. "Illegals" are Soviet officers who operate under non-official cover, often with false identities and appear to have no known affiliation with the Soviet Union. Monitoring illegal movement is virtually impossible in comparison to known "legals".

The primary KGB and GRU operational field element is referred to as the "Residency" and is located in a Soviet embassy or consulate in New York, Washington and San

Francisco. Recent estimates indicate there are approximately 2,100 Soviet diplomats in the United States and it is suspected that 30% are professional intelligence officers.¹² This massive hostile collection apparatus demonstrates the enormity of the counterintelligence problem and threat.

The KGB takes their business very seriously. The intelligence officer recruits for the First Directorate go to school for over a year just to learn the intelligence aspect of their profession. The KGB's First Directorate is located far from the center of Moscow in the suburban district of Yasenevo, in a building that looks very much like the CIA's headquarters at Langley, Virginia. The Foreign Intelligence School is more like a prison. It is a four story brick building surrounded by forest. It is patrolled by KGB officers 24 hours a day and by watchdogs as well. Its high walls are topped with barbed wire. The instruction in the classrooms is demanding and serious. Students start at 0800 and classes end at 1800.¹³

While our intelligence services also have formal instruction, it cannot compete with the thoroughness of the KGB. This needs to change if we are going to have a successful security policy. The Soviets are trained in surveillance, countersurveillance, the use of electronic devices, the use of psychological techniques and agent operations. They learn the methods used by the major intelligence and counterintelligence services and the professionalism and perseverance of the CIA. They put particular emphasis on recruiting spies, winning someone

over to the Soviet side, and maintaining a relationship between case officer and agent. This would start with an ordinary, even innocent, friendly contact. They measure someone's vulnerabilities, cautiously offer gifts, trap them, begin to exact favors, until the target is truly hooked. They are willing to offer money, women, drugs, blackmail and anything else to entice a potential spy. However, money is the current common denominator.¹⁴

IV. DOD SECURITY RESPONSIBILITIES

In order to appreciate the role of the Naval Investigative Service in counterintelligence and counterespionage it is helpful to have a general understanding of the overall Department of Defense responsibilities in these areas. The DOD intelligence community which includes such responsibilities as signals intelligence, imagery intelligence, scientific and technical intelligence and other non-HUMINT aspects are all important but do not necessarily involve spies.

The origins of U.S. counterintelligence and counterespionage can be traced back to the Revolutionary War. However, it was not until 26 June 1939 that the White House made a concerted effort to make a "community" for HUMINT collection. On that day the White House issued a confidential memorandum to the Secretary of State, the Secretary of the Treasury, the Attorney General, the Postmaster General, the Secretary of the Navy and the Secretary of Commerce, which read in part:

"It is my desire that the investigation of all espionage, counterespionage, and sabotage matters be controlled and handled by the Federal Bureau of Investigation of the Department of Justice, and the Military Intelligence Division of the War Department, and the Office of Naval Intelligence of the Navy Department. The directors of these three agencies are to function as a committee to coordinate their activities.

No investigations should be conducted by an investigative agency of the government into matters involving actually or potentially any espionage,

counterespionage, or sabotage, except by the three agencies mentioned above."¹⁵

Since the memorandum of 1939, numerous executive orders, public laws, DOD instructions and memorandums of understanding have guided the DOD intelligence community. Because of the sheer size of the military it should come as no surprise that DOD has the largest part of the intelligence community. Within DOD each military service has developed its own intelligence organizations. Numerous attempts have been made to centralize functions but each service has viewed this as an usurpation of their responsibilities. While all the services are centralized under the Secretary of Defense each has its own charter and respond in an autonomous manner. The DOD intelligence apparatus is made up of the National Security Agency (NSA), the Defense Intelligence Agency (DIA), the Intelligence Units of the Army, Navy, Air Force and Marine Corps, and elements within the Office of the Secretary of Defense.

Organizationally, each service has an element responsible for counterintelligence, counterespionage, counterterrorism and the investigation of espionage and security violations. Within the Department of the Navy this responsibility lies with the Naval Investigative Service. Appendix (C) depicts the Department of Defense Foreign Counterintelligence Management Structure. The Military Intelligence Community is a book that provides an excellent overview of the DOD intelligence apparatus.¹⁶

Before leaving the DOD overview it is important to understand that there are numerous checks and balances,

from congressional oversight committees to criminal statutes, that regulate the conduct security and intelligence collection and investigations. For the military, we must show a military connection before we initiate inquiries in the security arena. Additionally, we must coordinate with the Federal Bureau of Investigation for counterintelligence and espionage investigations in the United States and with the Central Intelligence Agency when the inquiries are overseas.

V. NIS COUNTERINTELLIGENCE

The Naval Investigative Service (NIS) is the primary agency within the Department of the Navy charged with the detection and neutralization of the espionage threat. "Its authority for conducting counterintelligence investigations and related activities is grounded in presidential directives and various Department of the Navy and Department of Defense instructions and agreements."¹⁷ The Federal Bureau of Investigation has primary responsibility for countering the domestic espionage threat. However, the NIS in conjunction with the FBI and Central Intelligence Agency abroad, conduct counterintelligence operations and investigations designed to identify and neutralize hostile intelligence activities as they impact on the Department of the Navy.

The NIS is organized into major departments including: Information and Personnel Security, Criminal Investigations, Law Enforcement and Physical Security Programs, supporting departments and the Counterintelligence (CI) Department. It is the Counterintelligence Department that develops, implements and manages the Navy's counterintelligence and counterespionage programs. The organization of the CI Department is reflected in Appendix (D).

The primary NIS operational office is the Naval Investigative Service Resident Agency (NISRA). There are more than 180 offices worldwide divided into ten regions.

Depending on the perceived threat, counterintelligence assets range from one agent to entire squads who offer a myriad of CI support. There are over 350 foreign counterintelligence agents worldwide for NIS.

During the 1980's the United States has witnessed a significant increase in the number of spies. The Navy was victimized by the Walker betrayal which by all accounts provided the Soviets a wealth of information and technological enhancements. During the last eight years NIS investigations have resulted in over 35 convictions by court martial or federal district court.^{1B} There truly does appear to be an increase in spying, or at least we are catching more of them. With the danger so real there is no doubt for the need of a strong counterintelligence and counterespionage effort by NIS.

The current strategy by NIS is a multi-disciplinary approach. Here are some of the programs in effect to combat espionage and counter Soviet intelligence efforts:

1. Double Agent Operations: This type of operation involves an asset under the control of one intelligence agency who offers his or her services to an opposing intelligence agency. Through the use of double agents (DAs) the intelligence community is able to identify hostile intelligence service (HOIS) operatives and agents, tradecraft (the technical gear used by the KGB), electronic and photographic eavesdropping capabilities, sources and methods of operations, and areas of interest or essential elements of information.

Another goal of DA operations is to discourage HOIS from accepting walk-ins who come to them offering their services. An argument to DA operations posed by the Navy is that NIS cannot guarantee the safety of the Naval DA. To some extent this is true, however, the risks observed by the counterintelligence agencies are small and Naval personnel, in all likelihood, would be able to carry on with the careers after the DA status.

2. NIS espionage investigations. These investigations entail the traditional investigative activity: visual, technical or electronic surveillance, mail covers, records review, interrogations and polygraph examinations. The primary objectives of these investigations is the elimination of the espionage threat and criminal prosecution.

3. NIS CI operations. This is a proactive organized effort by NIS to detect espionage and security related matters. These operations are developed by experienced agents and from other agencies successes.

4. NIS Passive Listening Post Program. This program involves the selection of Naval personnel at sensitive Naval commands. The Navy person is recruited and trained by NIS to be alert for any indications of espionage or pattern of serious security violations. The program does have some drawbacks. Understandably, it can look like "Big Brother" is watching.

5. Proactive Counterespionage Program (FACE). This program attempts to identify those DON personnel in a specific command who may be engaged in espionage utilizing

a series of actions to include: CI briefings (espionage awareness), criminal record inquiries, service and medical record reviews, reviews of command disciplinary and indebtedness records, identification of potential areas of compromise, facility security profiles, and interview of command personnel. These activities are intended to identify any known espionage indicators, sensitize command personnel to the espionage threat, and enhance the ability of NIS to service the command.

6. NIS preventive and defensive counterintelligence initiatives. This includes physical security, counterintelligence briefings programs, espionage hotline, Multi-Disciplinary Counterintelligence Analysis (MDCI), Operational Security (OPSEC) support to Navy special access programs, technical surveillance countermeasures (TSCM), port security, Anti-Terrorism Alert Center (ATAC), and the polygraph. Also within this strategy is the ongoing Navy effort to decrease the number of personnel who have access to classified information and to conduct damage assessment when there is a compromise.

All the above actions by NIS, or for that matter any other intelligence agency's efforts, have not stopped espionage against the United States. Who are the individuals committing espionage and why?

VI. REVIEW OF RECENT NAVY SPIES

The following examples disclose the magnitude of the threat espionage poses to the United States. Many have been highlighted in the press and will not be discussed in detail here. But one should gain a sense of the gravity of the situation when someone betrays their country. All of the examples are from the records of the Naval Investigative Service.¹⁹

A. Without a doubt the most damaging espionage against the United States was the Walker spy ring. The leader of the ring, John Anthony Walker, Jr., joined the U.S. Navy on 25 October 1955. While serving in the Navy, Walker was considered highly competent. He advanced through the enlisted ranks and rose to Warrant Officer and retired in 1976 as a Chief Warrant Officer. He had many duty stations and assignments, most of which required a security clearance. Walker had made some bad investments and was having marital problems and by 1968 he needed money. He went to the Soviet embassy in Washington, D.C. and offered his services for purposes of espionage. Walker provided the Soviets with key cards used for enciphering messages and provided the encryption devices themselves.

During more than 17 years of espionage performed on behalf of the Soviet KGB, Walker directly compromised numerous pieces of classified information and equipment to include the decryption keys, which in turn led to the compromise of over a million classified messages. Walker

became concerned over his security clearance and retired. However, he was making far too much money from the Soviets to let a good thing end so he recruited others into the network, including Jerry A. Whitworth, a Senior Chief Radioman who had served with him. Walker also recruited his own son, Michael L. Walker, who had enlisted in the Navy. John Walker also attempted to recruit one of his daughters who was serving in the U.S. Army. A KGB defector said the KGB considered the Walker ring the most important operation in its history. The Walker spy ring was broken and caught because of an unhappy marriage. John Walker's wife, who had known for many years that he was a spy, eventually informed the FBI of his espionage activities. Numerous items of intelligence, classified documents and tradecraft equipment was seized as a result of the arrests. All three men were convicted in federal court and received heavy sentences.

B. Robert Ernest Cordrey, a U.S. Marine Corps Private, was an instructor at Camp Lejeune, North Carolina, Warfare School. In April 1984, Cordrey began phoning numerous embassies in an attempt to sell documents and manuals relating to nuclear, biological and chemical warfare. After several futile attempts, Cordrey made contact with a Czechoslovakian intelligence officer and he drove to Washington D.C. from Camp Lejeune for a clandestine meeting. Cordrey passed sensitive information and subsequently arrested and convicted for espionage.

C. Clayton J. Lonetree enlisted in the U.S. Marine Corps and in 1984 was posted in Moscow, U.S.S.R., where he

served as part of the Marine Corps Guard Detachment for the U.S. embassy. During his assignment in Moscow, Lonetree had an affair with a Soviet woman, Violetta Seina, who had previously been a telephone operator and translator at the U.S. embassy. Soon after their relationship began, Seina introduced Lonetree to her "Uncle Sasha" who was later identified by U.S. intelligence as being a KGB agent. In December 1986, Lonetree turned himself in and admitted to committing espionage which included providing the names of American intelligence agents to the KGB. On 24 August 1987, Lonetree was sentenced to 30 years in prison, fined \$5,000, lost all pay and allowances, was reduced to the rank of Private, and was given a Dishonorable Discharge.

D. Jonathan Jay Pollard was hired in 1980 by the Naval Intelligence Support Center where he worked as a Civilian Analyst. In 1984 Pollard was hired by NIS as a Terrorism Analyst. In early 1984 Pollard requested a meeting with an Israeli military officer. A meeting was effected in the summer of 1984, at which time Pollard agreed to pass classified information to his Israeli contacts. Pollard would take classified documents from the NIS headquarters, make photocopies and provide them to his Israeli contact. He passed enormous amounts of material and was paid handsomely for his efforts by Israel. Pollard was arrested on 21 November 1985 after his suspicious activities were noticed and reported by a co-worker.

D. Unfortunately, the list could go on far too long. Individuals like: Michael H. Allen, Stephen Anthony Baba,

Nelson C. Drummond, Wilfredo Garcia, Stephen D. Hawkins, Brian P. Horton, Samuel L. Morison, Brian Everett Slavens, Michael Timothy Tobias, Edward Hilledon Wine and Hans Palmer Wold, all committed or attempted to commit espionage.

There are several common denominators for all these men. They were all connected with the Navy, either civilian or military, all had access to classified information and/or documents, all were considered good to outstanding performers, and all of them attempted to or sold out their country for money.

VII. FUTURE COURSES OF ACTION

We should begin our strategy by recognizing that spying is a fact of life. We know we are being targeted and we know that certain individuals are willing to betray our country for monetary reasons. NIS agents are highly motivated and want to do the best job for the Navy and our country. We can do better. We must do better. The following recommendations could provide the framework for a more effective policy to combat espionage:

1. The multi-disciplinary approach is the correct avenue for an overall effective program for keeping the Navy's secrets. In this so called era of "Glasnost" the Soviet Union, its surrogates, and other countries with interest adverse to the United States, are expanding their massive and highly organized intelligence operations against DOD personnel. In order effectively to thwart their efforts toward the Navy, NIS must receive a substantial increase in assets for the counterintelligence and counterespionage programs. With slightly over 350 agents to cover the world-wide CE/CI mission for the Department of the Navy, an overall and comprehensive program is just not possible. The key to getting these assets is a high profile, vigorous public information campaign along with an increased DOD and congressional liaison effort.

2. Along with increased assets NIS must coordinate with SECNAV, CNO and ONI to identify high threat targets to HOIS and devote manpower to these areas.

3. Our training must be enhanced. Remember, the KGB trains its agents for over a year in the art of espionage and intelligence collection. Current NIS training is narrow in scope and coverage. It is not mandated by any intelligence oversight committee, Navy regulations or formal NIS headquarters policy. Unfortunately, agents can be dedicated to CI/CE billets with little or no formal training. This hurts our professionalism and degrades our assets in the field. In particular, we must improve our interview and interrogations skills, countersurveillance abilities, and covert use of human assets.

4. NIS field offices should coordinate early on with their Staff Judge Advocates and Judge Advocate General Corps counterparts regarding CI/CE investigations to ensure effective resolution, both in terms of investigative coverage and successful prosecution. From a headquarters perspective, these two units can continue to advocate for stronger legislation (both federal and military) to enhance criminal enforcement and prosecution remedies.

5. Because of current taskings, there has been little time for research and basic analysis of our current strategy. We need to substantially increase our planning, research and development and analysis of our CI/CE strategy. A support division within the CI Directorate may be needed to cover the wide range of security related issues.

6. With the assistance of DOD, Congress, and Presidential supports, we need to increase the use of

counterintelligence scoped polygraph examinations. We should require that continuing access to classified information subjects personnel to the polygraph. Even the possibility that an individual may be subject to a polygraph examination will provide a powerful deterrent to those who might consider espionage.

7. There is a need to get commanding officers, civilian managers and all of Navy management on board to support the NIS CI initiatives, particularly the sensitive and controversial programs like polygraphs, passive listening posts, and double agent operations. This may have to be directive in nature (i.e., SECNAV instructions), but it should be achieved by good salesmanship by the NIS management at headquarters and their supervisors in the field. These supervisors also need to be sold on the NIS CI strategy so they will be able to convince senior commanders of the importance of cooperation in this common goal.

8. NIS should develop a "Psychological Operations Program" that induces and reinforces attitudes and behavior favorable to our objectives of sound security and detection of spies. This program could include unannounced security inspections, increased random searches, unannounced polygraph examinations for those individuals holding clearances, and increased visibility of NIS and command assets emphasizing a sound security program. These and other measures would instill in the minds of all personnel that if they attempt to spy they

will be caught. There is currently no training in any of the aspects of psychological operations.

9. The arms control treaties between the United States and the Soviet Union will also affect the NIS's counterintelligence efforts. The permanent Soviet presence and monitoring of some of the Navy's most sensitive areas will allow unprecedented collection opportunity. NIS must effectively address the numerous counterintelligence problems stemming from the Soviet presence sanctioned by the treaties.

10. There is a need for a countersurveillance program at overseas bases to determine not only the CE/CI threat but also to counter terrorism. The Navy, through an NIS program in countersurveillance, could train select personnel to observe unusual activities and suspicious individuals around military installations and gathering places of service members. The objective of this program would be to thwart hostile collection activities and potential terrorist acts against U.S. Navy interests.

VIII. CONCLUSION

"While the Soviet obsession with secrecy often irritated me, the western--particularly the American indifference to elementary security rules struck me as dangerously careless."²⁰ That quote, by a Soviet diplomat who defected to the United States, quite accurately summarizes our problem. We are a free and open society, and as a nation we want to retain our freedom. From an intelligence and security standpoint these ideals, which we all cherish, makes catching spies all the more difficult. We have seen the threat and examined how they train to attack our vulnerabilities. We have looked at the people who sold out their country for monetary gain and we have looked at the NIS efforts to combat the threat.

While no strategy of security can provide foolproof protection against espionage, it can make espionage more difficult to undertake and more difficult to accomplish without detection. We need to increase our efforts in the security arena. Almost all of the recommendations presented in this paper have a price tag on them. But, as the saying goes, "you can pay me now, or you can pay me later". Of course, later will be when new headlines hit the press about another Navy spy. This is not a "gee-whiz" article extolling the virtues of NIS. It is an article that describes a very real threat and the NIS effort to thwart it, but more importantly offers some new

and untried methods for seeking out spies that are surely in hiding.

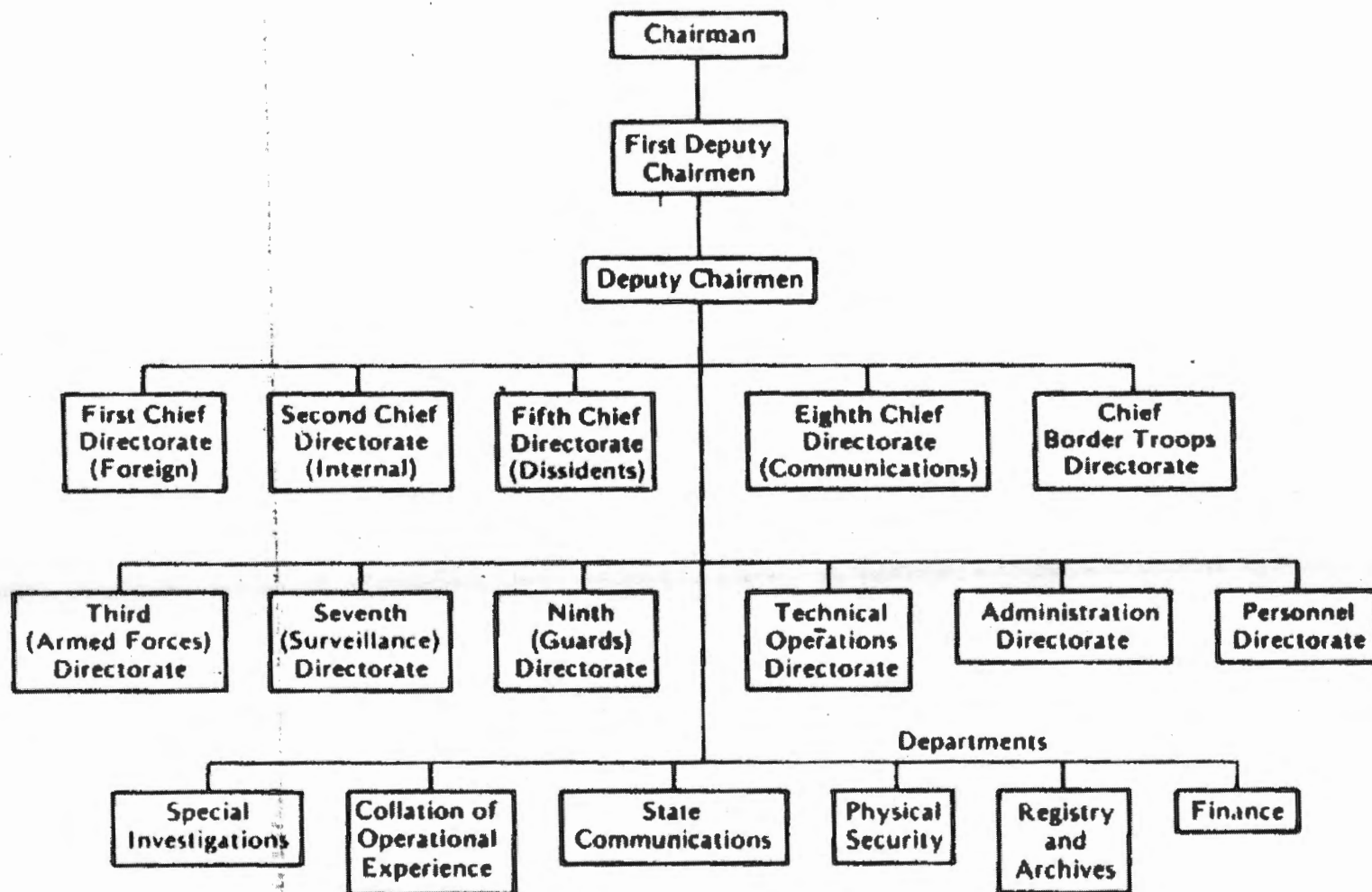
Security plays an important supportive role for the overall mission and strategy for the Department of Defense. If we do not pay adequate attention to this role we are destined to Fogo's aphorism: "We have met the enemy, and he is us."

The introduction of this paper described the 1980's as the decade of the spy and indicated that as a nation we could not afford a repeat in the 1990's. Unfortunately, the outlook is dismal for the U.S. Navy. According to records of the NIS headquarters the following service members have been convicted in court for espionage and security related matters since January 1990.

Francis H. Fequa, OMC (SS) USN	(Jan 90)
Gregory S. Loy, ISSN USNR	(Feb 90)
Elgin D. Thomas, YNCS USN	(Mar 90)
Charles E. Schoof, OS3 USN	(Apr 90)
John J. Haeger, OS3 USN	(Apr 90)

Are there more spies in the Navy or are we just doing a better job of catching them? The question goes unanswered but one thing becomes perfectly clear, we must pursue an aggressive counterespionage and counterintelligence program to protect the nation's security and freedom.

ORGANIZATION OF THE KGB

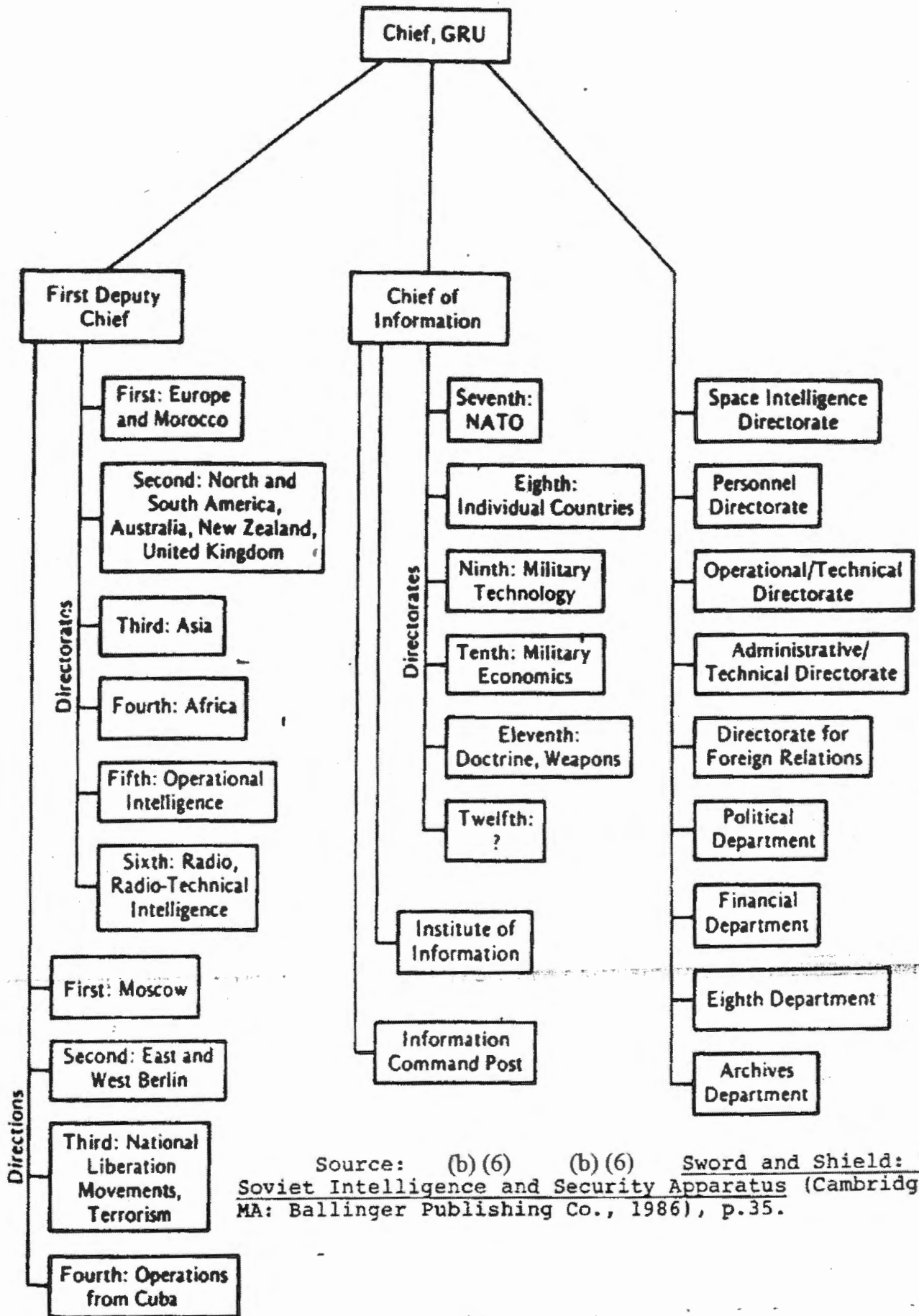


29

APPENDIX A

Source: (b) (6), (b) (6), Sword and Shield: The Soviet Intelligence and Security Apparatus (Cambridge MA: Ballinger Publishing Co., 1986), p. 22.

ORGANIZATION OF THE GRU
APPENDIX B



Source: (b) (6) (b) (6) Sword and Shield: The Soviet Intelligence and Security Apparatus (Cambridge MA: Ballinger Publishing Co., 1986), p.35.

**DEPARTMENT OF DEFENSE
FOREIGN COUNTERINTELLIGENCE MANAGEMENT STRUCTURE**

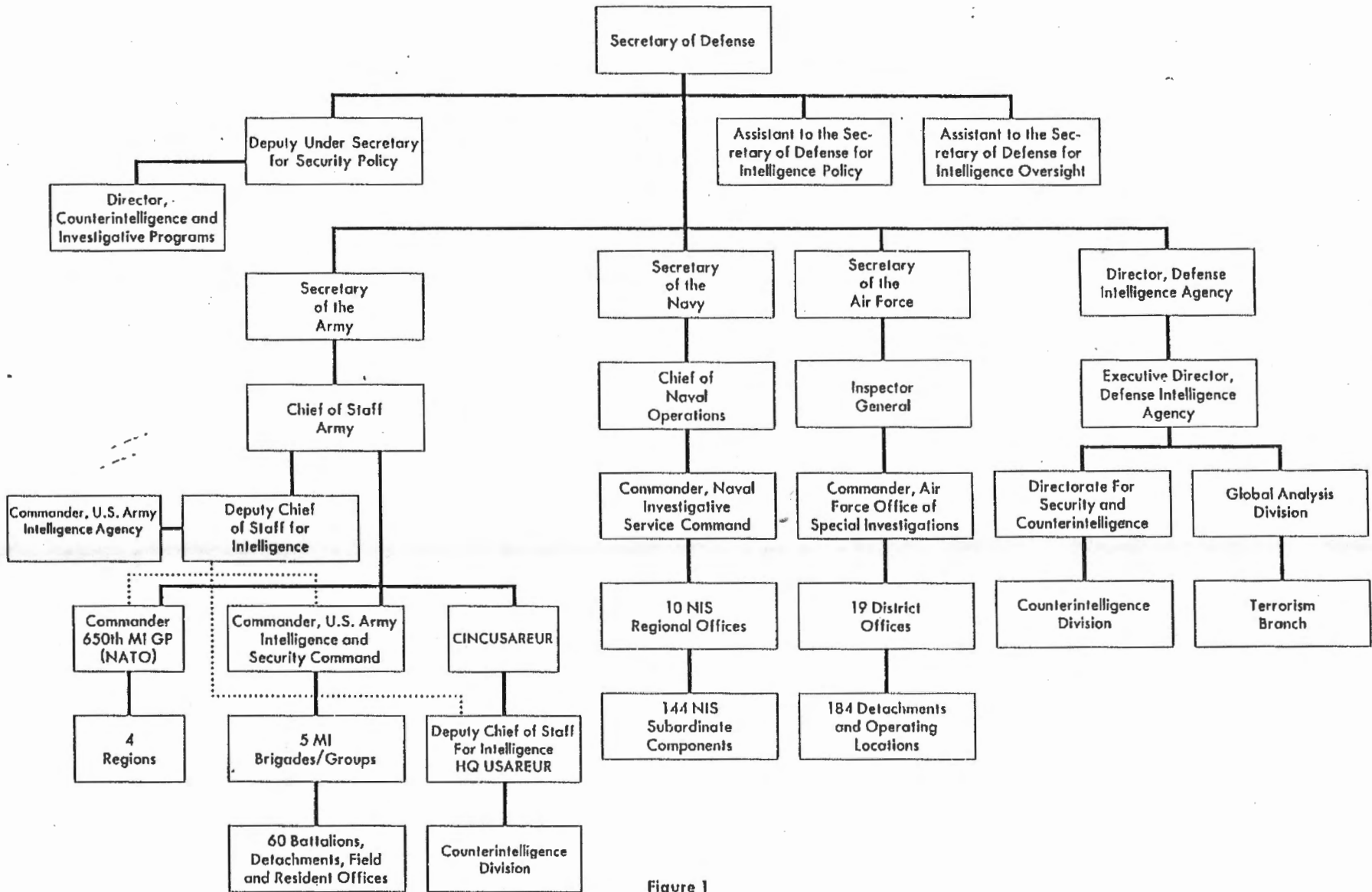


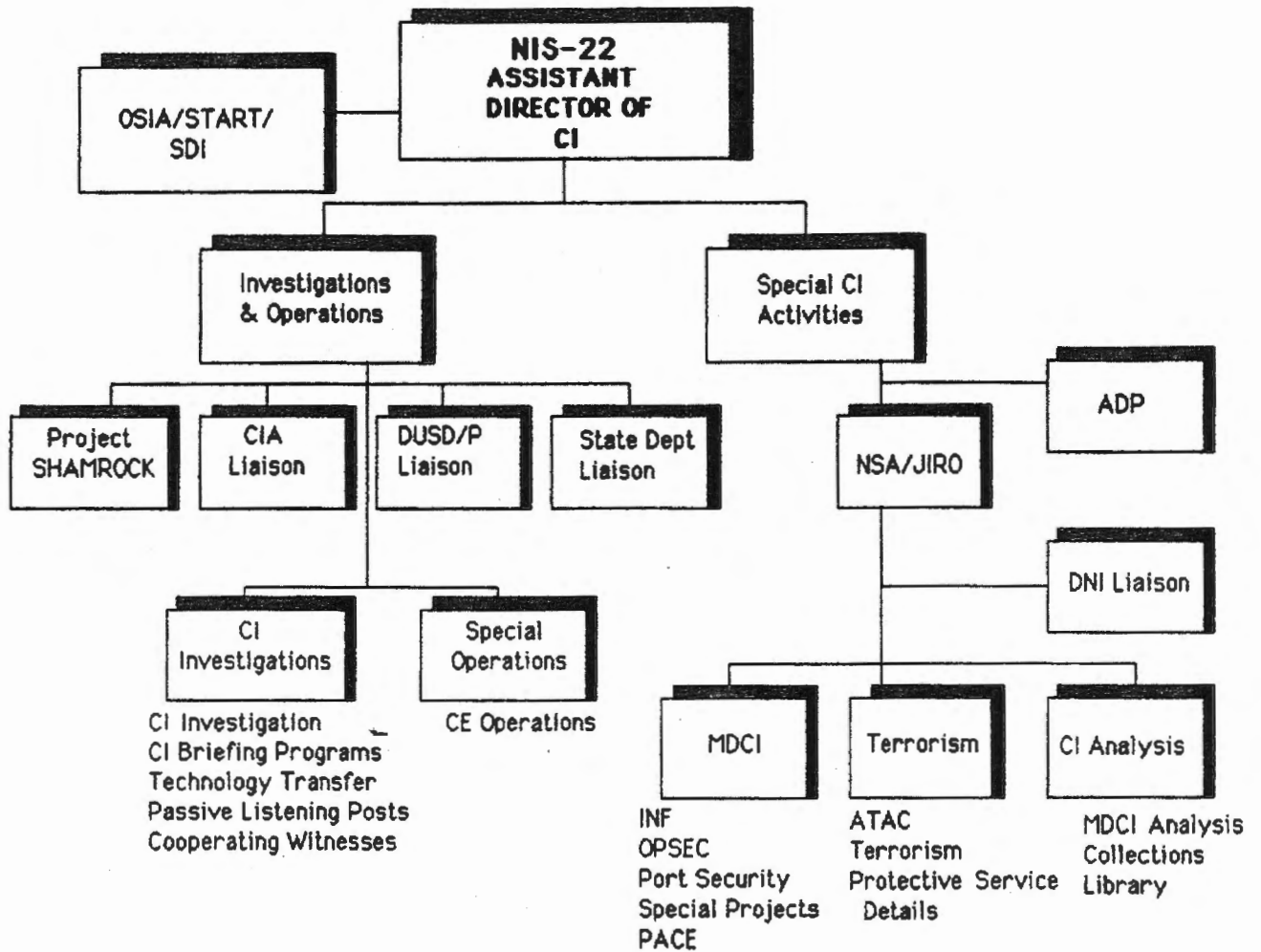
Figure 1

31

APPENDIX C

NIS COUNTERINTELLIGENCE DEPARTMENT

APPENDIX D



NOTES

1. U.S. Naval Investigative Service Command. Espionage, Staff Report (Washington: U.S. Government Printing Office, 1989), p. 19.
2. Statement of RADM Thomas A. Brooks, U.S. Navy, Director of Naval Intelligence, Before the Sea Power, Strategic and Critical Material Subcommittee of the House Armed Services Committee on Intelligence Issues, 22 Feb 1989, taken from The United States Naval War College, Operations Department, NWC 2269, p. 2.
3. Ibid., p. 22.
4. (b)(6) ⁰⁰ On The Wrong Side: My Life in the KGB (McLean, VA: Pergamon - Brassey's, 1988), p. 234.
5. Ibid., p. 234.
6. Ibid., p. 237.
7. (b)(6) (b)(6) 1, KGB: "The Secret Work of Soviet Agents," (New York: Reader's Digest Books, 1974), p. 468.
8. Ibid.
9. (b)(6) ⁰⁰ (b)(6) Breaking With Moscow (New York: Alfred A. Knopf, 1985), pp. 290-326.
10. (b)(6) (b)(6) Sword and Shield: The Soviet Intelligence and Security Apparatus. (Cambridge, MA: Ballinger Publishing Co., 1986), pp. 30-32.
11. (b)(6) , p. 242.
12. U.S. Naval Investigative Service, Manual for Counterintelligence Operations, (Washington, 1987), pp. 1-2.
13. (b)(6) , pp. 75-79.
14. Ibid., pp. 80-81.
15. U.S. Naval Investigative Service Command, Espionage, p. 2.
16. (b)(6) (b)(6) The Military Intelligence Community (Boulder, CO: Westview Press, 1986).
17. U.S. Naval Investigative Service, Manual For Administration. (Washington, 1985), pp. 1-1.

18. U.S. Naval Investigative Service Command,
Espionage, p. 34.

19. Ibid., pp. 5-23.

20. (b)(6) , p. 229.

BIBLIOGRAPHY

- (b) (6) . Merchants of Treason. New York: Delacorte Press, 1988.
- (b) (6) . Breaking the Ring. Boston: Houghton Mifflin Company, 1987.
- (b) (6) (b) (6) KGB: The Secret Work of Soviet Secret Agents. New York: Reader's Digest books, 1974.
- (b) (6) (b) (6) (b) (6) . The Military Intelligence Community. Boulder, CO: Westview Press, 1986.
- (b) (6) . Spy vs. Spy. New York: Charles Scribner's Sons, 1988.
- (b) (6) . Family Treason (The Walker Ring). Briarcliff Manor, New York: Stein and Day, 1986.
- (b) (6) . On the Wrong Side: My Life in the KGB. McLean, VA: Pergamon - Brassey's, 1988.
- (b) (6) Sword and Shield: The Soviet Intelligence and Security Apparatus. Cambridge, MA: Ballinger Publishing co., 1986.
- (b) (6) Breaking With Moscow. New York: Alfred A. Knopf, 1985.
- (b) (6) Inside Soviet Military Intelligence. New York: Macmillan Publishing, 1984.
- U.S. Congress, House Select Committee on Intelligence. Compilation of Intelligence Laws and Related Laws and Executive Orders of Interest to the National Intelligence Community, as amended through Mar. 1, 1987. Washington: U.S. Govt. Print. Off., 1987.
- U.S. Department of Defense. Keeping the Nation's Secrets: A Report to the Secretary of Defense by the Commission to Review DOD Security Policies and Practices. Washington: 1985.