IDENTIFYING THE TRAITOR AMONG US: THE RHETORIC OF ESPIONAGE AND SECRECY

by

Karen M. Taylor

BA Tulane University, 1993

MA Texas A&M University, 1996

Submitted to the Graduate Faculty of

Faculty of Arts and Sciences in partial fulfillment

of the requirements for the degree of

Doctor of Philosophy

University of Pittsburgh

2003

UNIVERSITY OF PITTSBURGH

FACULTY OF ARTS AND SCIENCES

This dissertation was presented

by

Karen M. Taylor

It was defended on

May 20, 2003

---

and approved by

Ted McGuire

Lester Olson

Kirk Junker

John Lyne

Dissertation Director

IDENTIFYING THE TRAITOR AMONG US:
THE RHETORIC OF ESPIONAGE AND SECRECY

Karen M. Taylor, PhD

University of Pittsburgh, 2003

This study approaches espionage as a knowledge-producing and knowledge-disseminating practice similar to knowledge practices such as science. The study uses investigative tools drawn from rhetoric of science studies and applies them to intelligence and, particularly, counterintelligence work. The result provides new insight into the underdetermination of evidence, the interdependence of disparate discourses, and the role of espionage in American culture.

TABLE OF CONTENTS

Espionage is a popular topic to write about these days. Roughly three hundred million spy novels are sold every year[1], enough to merit a significant amount of shelf space at your local Barnes and Noble. Clancy, LeCarré, and Fleming are only a few of the authors who have made a living writing about espionage. The situations and the character of the spies vary widely, but all share common themes of secrets and man's relationships with governments (both his own and foreign governments). And writing about America's better-known spies, from journalists and from biographers, has attracted many additional scribes. To take one example, the recent Robert Hanssen espionage case resulted in a television drama, at least two books, and over 300 newspaper articles. Over sixty-five spy biographies and/or histories of real-life spies have been published in the last three years alone. In a recent month (February 2003), there were at least 27 hours of espionage-related programming on television, ranging from history channel explorations of civil war espionage to science-channel programming on the new unmanned spy planes being tested in practice for the first time in Iraq today.

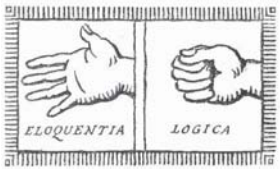
The popularity of the topic has a lot to do with the current political situation in the United States. As part of the "War on Terror" President Bush has strengthened the role of intelligence, both foreign and domestic. The CIA, NSA and FBI have all been hiring constantly since 9-11, adding 3000 new agents to their combined ranks in the last two years. The powers of the intelligence agencies have also been increased. The laws preventing the CIA from using known terrorists as informants have been quietly revoked. The laws preventing the FBI and local police departments from sharing information have been revoked, though less quietly. If it stands, a New York District Court ruling will allow law enforcement agencies to spy on political groups

[1]According to Book Magazine, July 2001 issue.

without need for a warrant or in relation to any particular criminal investigation. And agencies which were never considered part of the work of intelligence previously have become involved. Secrecy has grown more dramatically than under any other president. At the beginning of Bush's presidency, eight government agencies had original classification power. Today, eleven agencies have classification power, and even more strikingly the number of individuals employed by those agencies (and hence needing security clearances) has increased even more dramatically, such that at the start of the 1990s there were more than three million individuals with security clearances. The number of classified documents accompanying that increase in personnel, inevitably must therefore increase still more rapidly. And inevitably, with a dramatic increase in secrecy, an increase in instances of espionage is likely to accompany the change.

ESPIONAGE AND RHETORIC

Espionage is indirectly a topic that has been of interest to rhetoricians as well as to popular audiences. Rhetoric has a long and glorious history of championing open communication. In any situation where the secrecy/disclosure polarity arises, rhetoricians can be relied upon to argue eloquently the merits of open discourse. The tradition goes much further back than Habermas. Ed Black makes reference to the paired images of rhetoric and philosophy in Medieval art, Rhetoric with her hands open and outstretched and Philosophy with a closed fist, grasping for Truth.



The secrecy/disclosure continuum shall be the central focus of my research, and in particular the manifestation of this tension in its most dramatic form–espionage. Espionage is dramatic in the sense of lending itself to literary conventions, as well as riveting public attention. The term espionage carries with it as well associations with a number of closely related terms, each of which has emotional connotations and needs to be defined in relationship to the key term of espionage. The term espionage, as a sign, also necessarily references "silence" and "secrecy."

Espionage is a violation of secrecy, which in turn is preserved through silence. "Silence" here becomes a normative term, the preferred value in this pairing of opposites.

As with any contrastive pair (individual/society, stability/change, public/private), the middle ground between secrecy and disclosure is contested and hence the realm of rhetoric. The ascendancy of one term over another changes according to contexts and audiences. The context of World War II provides an example in which secrecy was relatively dominant, as reflected in the popular phrase "loose lips sink ships." The post-Watergate American audience in many ways represents an example in which the value of disclosure is rated more highly than the value of secrecy[2]. Entering into today's context we seem to see the secrecy/disclosure pendulum swinging back in favor of greater secrecy. The NSA, for example, has instituted a PR campaign to encourage secrecy.

Secrecy and silence are longstanding themes in the discussion of democracy. Anna Quindlen in Newsweek (4/21/03) notes, "In a democratic society, the only treason is silence." Mills and Bentham, theorizing how democracy can function most effectively, both note that accountability (vital in a representative democracy) would seem to require first and foremost the availability of information, in order for the public to make informed judgements. Jürgen Habermas takes this requirement of complete openness as an ideal ethically and functionally. In practice, complete openness has never been possible or even purely desirable. Sissela Bok notes that secrecy in order to protect the right to privacy of individual citizens is as fundamental and

[2]For one manifestation, notice the amount and the type of information which formerly would have been considered "private" and hence appropriately secret which today is routinely exposed in the media. Other manifestations include the importance of "candor" or "sincerity" in ethos for presidential candidates.

traditional an ideal of our government as openness. The right to vote in private (that is, for your vote to be secret) was safeguarded in the constitution and at every other juncture, in all the ways possible. Similarly, secrecy regarding foreign correspondences has been a norm from the beginning, though it was referred to as "discretion," a euphemism still in widespread use.

This still leaves a question about the relationship between espionage and secrecy, which we need to address before understanding why a rhetorician is tackling the topic of espionage. What is a good working definition of espionage? Webster's dictionary tells us that espionage is "the art or practice of spying or using spies," but this definition is circular. A better definition can be found if we turn to the body of literature sociologists have built up on the topic. Nachman Ben-Yahuda approaches espionage from the perspective of criminal sociology, and he notes that "treason against a collective that is committed in secret tends to be labeled espionage" (p. 105). This definition calls our attention to two of the words most necessary to understand espionage, specifically "treason" and "secrecy." This definition is derived from studying cases across multiple societies that get labeled espionage. The definition also explains why covert action also has been placed under the purview of intelligence agencies in the U.S., because both espionage and covert action emphasize secrecy and the ability to pass as insiders while working against the targeted government. But covert action is unlike espionage in many ways, and therefore it will not be considered further in this project.

Espionage is a crime that today gets defined functionally in relation to the activities of the various intelligence agencies. Understanding espionage necessitates understanding the organizational context in which it occurs. Espionage could be most succinctly defined as sharing intelligence outside of the authorized community. This definition begs a number of questions. Who is this authorized community? This question will be addressed at greater length in the Ames chapter. And what exactly is intelligence? This question is one which has no settled answer. The legislation creating the intelligence community defines the term so broadly as to be

meaningless, stating that intelligence is "any information relating to people, places, things, events or actions of or related to foreign powers which might assist decision-makers in planning future courses of action." A clearer definition would need to reiterate the relationship between intelligence and secrecy, and between intelligence and analysis. A recent debate attempting to define intelligence can be found in the CIA's in-house journal, in a January 2002 issue dedicated to this question.

Espionage is a political crime, in the sense that it impacts groups, either governments or businesses rather than individuals. Espionage is a political crime also in the sense that what counts as espionage is defined by means of a process that is political, contentious, derived from and derivative of power. Power enters into the definition of espionage at two points in particular. Determining what information should be classified is a political decision. Since the creation of the classification system, every new president has issued an executive order laying out the new policy for what should be classified and how classified material should be handled. For example, President Carter issued an executive order declaring a statute of limitations on classified information, such that after 25 years information would be reviewed for release. President Clinton's executive order setting classification policy changed that to 15 years except in agencies dealing with nuclear-related materials, and removed the need for review. Instead the policy maintained that the information declassification was to be automatic rather than subject to review, though reviews could be instituted and could conclude that declassification should be pushed back by an additional 10 years. President Bush, in the recently-released Executive Order #12958, revoked the automatic declassification, and stated that in Freedom of Information and Privacy Act (FOIPA) cases the preference was to be in favor of maintaining secrecy. In other words, if any argument could be made as to why release of information might be damaging under any of the nine criteria, then the information must not be released. The political nature of decisions regarding classification can also be seen in studying the Legislative branch's

interventions into control of information. The FOIA and PA acts, passed in 1974, represent an attempt to wrest control of classification decisions out of the control of the executive branch. The other point at which espionage is most clearly a political crime is the decision to prosecute, and the question of what exactly the crime will be defined as. The Department of Justice, part of the Executive branch of government, makes the decision of which cases and how to prosecute. The general label of "espionage" is used to categorize together a number of crimes which are related but not the same. "Mishandling of Classified Information" is a different crime from espionage, and "Negligence of Duties" or even "Gross Negligence," such as the current case that has embroiled the head of Lawrence Livermore's counterintelligence program and another FBI agent who were both lovers of a suspected Chinese double-agent, are not the same crime legally as espionage, or conspiracy to commit espionage.

Political crimes are rhetorical by their very nature. Espionage is a particularly rhetorical example of a political crime, because espionage is communication. Espionage is nothing more than symbols passed from one individual to another. Espionage is a special type of communication only in that it has been forbidden. The forbidding is determined by someone in power who believes that the communication would have material results, and that those results would be inimical. There is a wide range of reasons and means by which this could be decided. Is the determination an attempt to control a pre-existing communication, usually a text that is either written or visual? Defining it in this way leaves some cases outside the definition which perhaps we would want to prosecute because of their clear nature as political crime. For example, there is a current case of a South Korean residing in California selling documents to the North Koreans. Is it espionage even though the documents are publicly available, such as lists of government officials and reports of trials? Or perhaps is espionage to be defined by controlling an abstract idea, the "information" behind the communication that is forbidden or even the very notion of selling information to an enemy? Both definitions are problematic. The determination

of results as inimical is also problematic, and has been approached in a variety of different ways. Because of the range of ways in which espionage has been defined, and the range of activities that have been classified under this label, it makes sense to briefly consider the history of espionage. The history of espionage shows us that alternatives to the definition currently in use are possible. Moreover, the previous uses of the term do not vanish utterly. Previous meanings are retained as layers of meaning available for influencing interpretation. For example, today espionage has two major types, corporate espionage and international espionage. Corporate espionage builds upon the previous meaning of the term in that again it represents communication that has been forbidden, but it is not a political crime. Corporate espionage is not treasonous, which has historically always been part of the meaning of term, because assuming loyalty to a company just because at one point they paid you for your labor is a meaning that relies on a whole set of norms and values that have only recently developed and only in capitalist societies. International espionage has always been defined as a type of treason, one which deals with the communication of information that one country wants to keep secret. This dissertation will only address espionage in one particular country, because this particular political crime differs hugely across countries. But first it is worthwhile to consider some of the variation in the meaning of this term across different contexts, before focusing narrowly on the current American context. Therefore I have included here a brief history, to demonstrate the variation of meaning over time and the ways those previous definitions impact today. I have also included here a brief history of the American context, because the differences between the American use of the term and that in other countries is shaped by that history.

American History

Spy scandals are relatively new in America. This is not to say that there were no spies in America previously–obviously every war produces a need for intelligence-gathering and hence a need for spies, even if they are not referred to as such. For example, in the American

Revolution, George Washington gained a reputation as an exceptional "spy-master," with extensive courier systems that reported to him personally and exclusively. On the opposite side, the famous traitor Benedict Arnold was a Loyalist who engaged in subterfuge, rather than openly opposing the rebels, and gained access that otherwise would have been protected against him. The lack of disclosure is what merited the label of treachery, not his opposition, which was in fact not unusual. Similarly, during the Spanish-American War and during the Civil War mechanisms were developed to gather information about the troop movements and policies of the enemy.

Two crucial differences create a context today which is wholly unlike that of earlier American history. One difference is that today even during times of peace and even with neutral or supposedly allied countries we engage in continuous intelligence collection. As a corollary which most citizens assume to be inevitable, we therefore now engage in continuous secrecy. This was not the case historically in America. Naive though it sounds today, the policy was best stated by Secretary of State Henry Stimpson's indignant declaration "Gentlemen do not read each others' mail." Undoubtedly our ambassadors to foreign nations were expected to keep their eyes and ears open for any information that would benefit the U.S., but this was done openly and unsystematically. The second crucial difference is that since World War I, and increasingly more so with World War II and the Cold War, laws were created to specifically regulate the flow of information. In 1917 the first such American law, the Espionage and Sedition Act, was passed, which made it illegal to pass "detrimental" information to an enemy or attempt to influence U.S. citizens in ways that would benefit an enemy during times of war. The Espionage and Sedition Act was seen as necessary because of the "fifth column" in Spain, which had significantly impacted that country's participation in the war efforts. Additionally, the Act enabled the government to suppress dissent against the war. Later the Act was extended to include times of peace as well, and grew to specify more precisely the crimes and penalties

included. In prescribing penalties, only in 1946 was the death penalty introduced as an option for sentencing. The reasoning behind this specification is curious; "treason" has always been eligible for the death penalty (and during times of war, the penalty was applied frequently by military tribunals. Today we would probably consider these executions to have been without benefit of what we would consider a fair trial). In the 1946 amendment to the Espionage and Sedition Act, the language is phrased as "to be sentenced to a penalty of death, or fines not to exceed $100,000, and/or prison not exceeding thirty years."

Even after the 1917 Act was passed, no trials for espionage per se were held until World War II, though numerous criminal trials and convictions were held for "conspiracy" and "sedition." The numerous trials included the use of the Sedition law to jail union leaders and Socialist Party activists. The "sedition" half of the law was successfully contested, with rulings that limit and clarify the language involved and set clear precedent. The espionage half of the law has had fewer trials, hence has fewer precedents and less clarity. Halperin and Hoffman in 1977 went so far as to say "The current espionage laws are in a state of total confusion. They form no coherent structure, and each part of them poses many complicated problems of interpretation. Neither the intended meaning nor even the literal meaning of the terms of each statute is obvious." (p. 107, Top Secret) The right of the government to classify information–a necessary first step in making espionage a crime–has never been forced to be substantiated. On what grounds does the federal government control the flow of information? What information have they the right to control? This question becomes particularly problematic with the creation in 1946 of the Atomic Energy Commission, which specified that no matter what the conditions of knowledge production might have been–privately funded, developed in collaboration with another country, anything–knowledge relating to atomic energy was automatically classified by the U.S. government and as such sharing such knowledge would be considered criminal. The AEC included the phrase "born secret" in reference to any knowledge related to nuclear science,

creating a unique situation in which any information related to nuclear science does not need to be actively classified. Rather, it is classified a priori, before the information is even developed. To prove that espionage occurred requires proving that a foreign government now possesses some nuclear information, hence disclosing the information itself in an open court, and that they received it from a particular American. This "born secret" clause also means that scientists engaged in related research, whether funded by the government or not, are impacted by classification issues that they might or might not be aware of, and for which they have not previously given consent[3]. What are the limits on the mechanisms the government can use to control the information? Curiously, this is one of few provisions of the law that have been challenged, based on previous British law that forbade "prior restraints" on publication but allowed penalties to be assigned after publication of state secrets, a provision which was struck down so that prior restraint is allowed if national security would be harmed. Given that from the beginning the public contested government secrecy based on politicians' privacy (The Free and Open Press), it is curious that the right of the government to control information garnered about other governments has never been challenged.

Within the context of the Cold War, espionage assumed a much greater public significance. The primary theater of the Cold War (and bear in mind that for the public mindset it was very much a war, with a dangerous enemy set to destroy us) *was* the "Great Game," a practitioners' euphemism for the world of espionage. This metaphor is significant, for it tells us several things about the perceptions of intelligence and espionage. "Great Game" is a telling

[3]It should be noted, in all fairness, that the government has to date always provided financial recompense to scientists whose work is deemed classified if they were not government employees.

metaphor. The first reference to it that I find is in the British Secret Service during World War I, but during World War II it becomes widespread among agencies engaged in intelligence-gathering and counter-intelligence. The notion of a "game" implies a set of mutually-agreed-upon rules, which we can see in the gentile recruitment efforts of one agency attempting to tempt members of a competing agency into espionage, and in the willingness of governments to exchange captured agents. The notion of a "game" also necessitates a winner and a loser, which the nature of information, particularly scientific information, does not normally imply. The metaphor also suggests a recognition about the lack of seriousness of the activity, a disconnect between the "game" and "reality." That a metaphor which appears to downgrade the importance of the profession should be coined by its practitioners and become the dominant description used by agencies across nations might seem surprising. A "game" metaphor suggests in one sense that it is not to be taken seriously, that it is only done for pleasure or in jest. The implication, given that the practitioners first coined the term, is that their work might be dispensable, an odd metaphor for them to have chosen. Another important implication of the "game" metaphor is that it follows clear rules, that the outcome is determined either by chance or the skill of the players, but can be understood at each step in terms of reference to mutually understood and agreed upon guidelines for practice. The result of such a metaphor can be seen in the gentile efforts of each agency to recruit the agents of the other over drinks, the mutual reinforcement of the importance and skill of the other.

Today the significance of intelligence work and therefore espionage persists, in spite of the many changes in the international context. The publicity involved with espionage cases is often out of proportion to the magnitude of the purported crimes. The metaphor of the "great game" might account for some of the popular interest. There is a sense that here we have individuals, not vastly different from you and me, making a direct and important impact on

national and international affairs through their own acts of bravery and cunning. Moreover, just as politics often gets reported in terms of a "race" or other simplified competition metaphor because it increases the drama, espionage and intelligence work generally lends itself to a sense of competition and high drama, with clear winners and losers. The popular interest is also fostered by popular fiction forms, which portray espionage as an action-adventure. The expectation that real-life intelligence work is similar to the fictional form is fostered deliberately by both practitioners and authors. Under Hoover, for example, the FBI served as consultant and source for both a radio show and later a television series glamorizing the work of FBI agents. Today the CIA has an office dedicated to serving as a resource for film makers and novelists, offering their services to provide insight into intelligence work with the belief that this will ensure "greater public awareness and appreciation of the agency's role" (CIA web page, www.cia.gov). Successful authors in the fictional genre almost all have first-hand experience in intelligence work. Clancy, LeCarré, Fleming, and such a majority of other successful espionage authors have direct experience that it has become a hallmark of the genre, one of the most distinctive (and oft-cited reasons for fans) characteristics that marks espionage fiction separate from related genres such as crime mysteries or war novels. For example, the work of David Stafford in "The Silent Game: the Real World of Imaginary Spies" details the close relationship by tracing changes in the genre across countries and over time, noting the constant close relationship between fiction and context. Similarly, the blurring of fictional forms with other textual documents has influenced our understanding of the history of intelligence work. As Peter Model points out in "The Spies Who Came in for the Gold," the memoirs published by agents are problematic from a historian's perspective because they are unverifiable and because audience expectations seem to shape the writing so that it universally conforms to genre forms.

Consideration of Significance Behind Popularity

Espionage is perhaps also such a popular topic because it allows us to explore crucial

issues in the relation between citizen and government, in a fictional form that simultaneously allows us to safely bracket the concerns being addressed. One of the characteristics of the espionage genre is that the hero (or heroine) is always an individual caught up in the mechanisms of government. This can provide both a sense of empowerment (the spy is able to influence events), but also (and in more recent developments in the genre, this is increasingly the case) can illustrate the ways in which government subverts the efforts of individuals. The agent discovers only layers upon layers of duplicity, both among the enemy but also within his/her own agency. Consider for example the most recent examples of Bond movies, in which "M" is discovered to be manipulating her agent by sending him on missions that are not what she initially pretends, and is discovered to be manipulating or manipulated by factions within her own (or the allied U.S.) government. The spy novel represents our opportunity to consider issues of loyalty and treason, trust and distrust, and conspiracy. Conspiracy theory is a constant in American culture. Mark Fenster in "Conspiracy Theories: Secrecy and Power in American Culture" points out that today the vestige of American populism often takes the form of conspiracy theories because of the distrust of the combination of secrecy and power that the intelligence role of government represents. Given the secrecy of not just the enemy government, but also our own government, how can the individual know whom to trust? Is it treason to betray your government if it does not seem to have the best interests of its citizens in mind?

Espionage novels let us explore, not just the relations between citizen and government, but also between citizen and others as part of a community. The theme of a spy novel is the search for secret information, most often the knowledge of a hidden traitor amidst the community of the loyal. Espionage is a betrayal of trust, and because "trust is considered to be sacred, the violation of trust is interpreted and reacted to emotionally" (Ben-Yahuda, p. 12). The hidden traitor "violates... on the collective level, a sense of an imagined community and of collective memories and national identities. Betrayal, therefore, breaches the symbolic moral

boundaries of some of the values we cherish the most–those we consider to be definitive in our moral hierarchies and priorities" (p. 27).

Spy fiction in the United States blurs with the reality of intelligence work particularly well because the history of our intelligence agencies has been the subject of high drama, and the agencies have been keen to exploit the popularity of the genre and deliberately blur the line between fact and fiction. The blurring benefits intelligence agencies in two ways. The Federal Bureau of Investigation discovered early that by turning the efforts of their agents into popular media forms, the popularity of the agency and in turn its funding, but even more importantly its power, were increased. The FBI was protected from criticism for most of its institutional history because of the secrecy of its work, because the intelligence collected included secrets that those in power wanted suppressed (for example, Hoover had files on the sexual habits of several Supreme Court justices, and assorted Congressmen and governors), and because the PR efforts of the agency, in encouraging radio and television series, made it too popular to attack even for a red-baiter such as McCarthy (even though the FBI for the most part did oppose McCarthy, whom they saw as ruining their chances to actually catch a Communist spy by attracting too much publicity to the hunt). The other advantage is one the CIA still takes advantage of today, in that by promoting awareness of fictional forms and letting those stand in for real intelligence work, the CIA attracts more applicants and also deflects attention from the activities in which the agency more routinely engages. It is not as exciting to talk about collection and analysis of images from satellites combined with intercepted but non-classified communication. So long as the agency regularly feeds high-drama stories such as stories about spies being caught, neither domestic nor foreign audiences will pay attention to such mundane tasks, which are in fact the major source of intelligence. The analyses are classified, but in fact the sources themselves are

not secret, merely downplayed by using the media and fiction as a cover and distracter.[4]

THE ORGANIZATIONAL STRUCTURE OF INTELLIGENCE

If we are to understand espionage rhetoric, it is necessary first to understand the organizational context from which it is produced. The constraints and resources available in rhetorical situations that call forth espionage rhetoric are based in the structures of intelligence work. Those structures include the legal context, the organizational context, current political contexts, and related discourses. Much of what follows here in this consideration of organizational context will be familiar to U.S. citizens who follow even cursorily any news outlets, because of the popularity of espionage rhetoric. Nevertheless, rather than assuming all readers will have this background knowledge, I will review here the essential organizations involved in intelligence work, and hence in espionage, in the U.S. For a more complete consideration, the classic volume by Henry Howe Ransom, while not updated to take account of post-9/11 changes, is the best resource.

In the United States, foreign espionage is primarily the purview of the Central Intelligence Agency, usually called the CIA. The CIA does not have exclusive responsibility for intelligence collection, and at many times since its creation in 1947 the CIA has been involved in power struggles with other U.S. intelligence agencies. Most famously, relations between the

[4]I have always been suspicious that the high-profile examples of intelligence agency blunders–we receive more reports of mistakes than of successes–are also part of a publicity ploy to downplay the capabilities of the agencies, so that domestic audiences don't become alarmed by their power and so that foreign agencies will not take them seriously enough to be as cautious as they should be. But I cannot prove that this is deliberate, and the same skewed emphasis can be seen with media coverage of space exploration.

CIA and the FBI, which has sole responsibility for intelligence-related activities in domestic territory, have often been strained to the point where cooperation proved impossible. The formation of the CIA established it explicitly in opposition against its competitor, the Defense Intelligence Agency (DIA), which was in its turn the offspring largely of the Navy's intelligence-gathering operation. The Defense Intelligence Agency continues to have separate operational branches, consisting of the Office of Naval Investigations, the Air Force Reconnaissance Operation, and the Army Intelligence Operation. The early history of the CIA created a setup that was fraught with problems from the beginning. The troubled history of the agency has constrained its intelligence work, because the agency was always secretive not just because of its mission but also because of the tensions between the CIA and other agencies of the government, including Congress, which nominally has oversight responsibilities. The mechanism of Congressional oversight is the Senate Intelligence Committee and the House Intelligence Committee, but historically much of the CIA's activity was exempt from review. Even the Executive branch has not always been fully apprized of CIA activity, though in the case of certain covert actions such barriers were deliberately maintained for the sake of plausible deniability.

Even the Executive branch which first created the CIA had concerns about the agency. "Truman's concern about the possible development of an American police state was the single most important factor in causing him to block early central intelligence agency proposals. In a meeting with Bedell Smith [from Budget Bureau, in charge of military reduction after WWII] on May 4, 1945, Truman instructed him not to enlarge that part of the presidential contingency fund used for foreign intelligence work and said 'with considerable vigor that he was very much against building up a Gestapo.'" (Rudgers, p. 40)

Alfred McCormack[5], an Army colonel and New York lawyer, was in charge of

organizing intelligence within the State Department at the end of World War II, and his opposition to continuing an active intelligence function is one of the primary reasons why the CIA today is a separate agency unconnected to any other cabinet-level branch of government. This separation has been one of the shaping constraints on the CIA, because it both enabled the maverick and secretive culture to develop, and also reinforced the paranoia that is characteristic of intelligence work because it meant that truly the agency did not have any allies in the government. In opposing creation of a unique and continuing intelligence function, McCormack stated, "I believe that research at the geographic level must be under the immediate direction of those who use it. In my judgement, the divorce of research from policy action taken after the evaluation of information will lead inevitably to wasteful duplication and to competing evaluations of information which will breed confusion and disorganize the operations of the Department....No justification can possibly exist for different geographic breakdowns. It would place the Department in a ridiculously inconsistent position to approve a geographic division for a new Office in the Department wholly different from that established and approved for the traditional offices of the Department[6]." State Department opposition appeared to be based partly on cultural differences of the sort expressed by Secretary of State Simpson, a belief that espionage is prima facie morally wrong. Opposition also seems to have been based partly on a belief that intelligence collection needed to be kept close to the policy-makers, not centralized. Any centralized intelligence group could coordinate, but not collect. Cultural opposition within State was also very real ("Culture shock" as Rudgers calls it, p. 47). Hence the opposition developed allying the Budget Bureau, the State Department, and the Justice Department against the Departments of War and Navy, who both wanted a central and active intelligence function. The FBI campaigned to take over the role themselves, but Truman was vehemently opposed, and the effectiveness of the FBI's track-record in Latin America, where they had operational responsibility prior to the end of World War II, was strongly questioned by both military and

Budget Bureau.

The military branches wanted a strong centralized intelligence agency, and preferred that it be organized military-fashion. Their arguments emphasized efficiency, in that there would be no danger of the duplication seen in WWII, and benefits of better coordination so that one secret agent wouldn't interfere with another, even accidentally, as had happened regarding the Manhattan project. The military branches relied then and continue today to rely less on keeping information compartmented and therefore secret even internally to prevent espionage. Instead the military relies on layers of classification, relying on discipline and harsh punishment of violators to prevent leaks of classified information to those outside the organization who should not have access to the information. The military branches had the greatest experience with intelligence at the time of the formalization of the intelligence collection function.

The Federal Bureau of Investigation was formed in 1911 in response to the growth of organized crime. Usually known by the acronym FBI, the bureau is responsible today for all domestic intelligence-related functions. The initial reasons for this division of labor were twofold. One argument was concern about protection of civil liberties. The sources and methods involved in intelligence collection that had been effective during World War II were deemed inappropriate for use against U.S. citizens. The FBI had also used its role in domestic intelligence collection, and the secrecy that was a corollary then and now, to increase its own power. The bureau had grown from its inception faster than any other federal agency, and was viewed when considering centralizing intelligence by other agencies, including the Post Office, the State Department, the military, and the Department of Justice which has official supervisory power over the FBI, as a threat needing to be checked. The power accumulated during J. Edgar Hoover's reign has been both a blessing and a curse for the FBI since that time. The FBI's history with abuse of civil liberties has left it keenly aware of the possibility of public scrutiny, which in turn shapes the ways in which it handles any espionage accusations.

Two other agencies today play an important role in intelligence-related activity. The Department of Energy, which is the successor of the Atomic Energy Commission that developed from World War II experience, has responsibility for all energy-related governmental activities. The DOE, as it is usually called, is thus involved in international issues such as forecasting our future oil consumption and ensuring that those needs will be met, developing alternative energy sources, and nuclear energy and weapons. The DOE's responsibility for nuclear weapon development, maintenance, and limitation places the agency into one of the most contested realms of intelligence work. Because DOE's responsibilities are mostly not intelligence-related, the organization's structure has evolved such that secrecy is much less central. DOE's organizational culture is more closely aligned with the culture of academic science than the inward-turned culture of an organization such as the CIA or FBI, whose responsibilities center around secrecy. It should not be surprising then that DOE is most often the site of overt clashes between secrecy and disclosure, and espionage rhetoric in the context of DOE is quite different than espionage rhetoric in intelligence-specific organizations.

The State Department also plays an important role even today in intelligence collection. The State Department is one of the primary recipients of intelligence analysis, a role which is referred to as a "consumer" of intelligence. The State Department is also a close ally of the CIA. The majority of CIA agents operating overseas do so under cover of the ambassador to the nation under investigation. Because CIA agents are officially employed by the State Department, they have diplomatic immunity, which can provide a measure of protection in most countries. The alternative, to enter a foreign nation by pretending to a false identity such as a businessman or tourist, places an agent in the category called an "illegal," and means that if he is caught he is subject to whatever punishment the host country chooses to mete out.

One final structural issue related to understanding espionage is the question of classification, which is the key to most of the legal constraints that have evolved in the U.S..

Classification systems also were not formally introduced until World War II. The United States has never passed a law equivalent to the British Official Secrets Act, which was also introduced in response to World War II. In Britain, any possession or unauthorized disclosure of any state secret is a criminal offense. Even during World War II, such sweeping legislation was not passed in America, though not for lack of trying on the part of senators such as Robert Byrd and Orrin Hatch. The laws governing classified material in the United States specifically forbid as criminal any passing of the information related to the national defense to unauthorized persons with the intent to harm the United States government. In the case of Gorin vs. U.S., the Supreme Court ruled that "related to the national defense" was not so vague as to be void, because the "intent" clause saved the law from being over-broad. The phrasing of this 1917 law necessitates that to prove espionage requires demonstrating intent to harm. Any other "mishandling" of classified information is not prosecutable as espionage, but can only be dealt with under the rubric of "mishandling" or "negligence," which carry much smaller penalties. The 1917 Espionage and Sedition Act resulted in a great many sedition trials, but very few espionage trials. The few that did occur, when German agents were discovered attempting to commit sabotage, were clear-cut and did not result in review by any higher courts. The first espionage trials that we usually think of as such, such as the trials of Judith Coplon or the Rosenbergs, were conspiracy trials. The crime for which these defendants were convicted was conspiracy to commit espionage, which tended to carry harsher penalties than simple espionage. The conspiracy laws, which had initially been crafted primarily to break the power of the mob, by imposing severe penalties and broad descriptions that would include a wide range of activities, were used as well to convict American citizens who had "conspired" with foreign governments against the interests of the United States. The fact that the conspiracy consisted of the sale (or giving away) of classified information created emotional drama, lent urgency to the proceedings, and justified some of the most extreme penalties possible. To prove a legal case of espionage

requires proving intent, and communication scholars are familiar with the difficulties of such a burden of proof.

The first trial to actually bring a charge of theft of classified information that was reviewed by the Supreme Court was not held until 1971. Ironically, the first case tried under our current espionage laws was the People vs. Daniel Ellsberg, who was charged in relation to the so-called "Pentagon Papers." The Pentagon Papers were the Defense Department's classified analysis of what had happened and what had gone wrong during the Vietnam War, and Ellsberg "stole" the information and gave it to The Washington Post. As his lawyer, Anthony Russo, noted, "This espionage charge is tantamount to arguing that the American people are the enemy of the American government."

THE LEGAL STRUCTURES OF ESPIONAGE RHETORIC

American espionage law is trying to strike a curious balance, and that's why the laws are changing continuously and why oftentimes cases are prosecuted under statutes that seem less than perfectly suited to the circumstances at hand. The "Espionage and Sedition" laws were not passed until our experiences with world wars. It's not that we didn't have a conception of treason before that, and our conception of treason would have included giving information to an enemy. In fact, treason is the only crime specifically mentioned in the Constitution, which concerned itself with limiting the definition of treason and requiring that the standard for the burden of proof was higher than had been the case in earlier societies by mandating that at least two witnesses were required to testify. The phrasing of the treason laws in the Constitution limited it to "aiding and succoring an enemy during time of war." Given this definition, it should not be surprising that the majority of treason cases were military, and the prosecution was usually a military tribunal, because generally only military employees would be in a position to break that law.

The tension in U.S. law arose because we want to ensure the safety of good secrets,

secrets that we want to keep secret, and to do that we want to be able to punish appropriately those who reveal good secrets. But at the same time we want to ensure that the government is not creating bad secrets, turning information that belongs in the public domain into a secret to protect specific individuals or conceal wrongdoing. There have been numerous arguments as to why secrecy is so harmful for a democracy, and given those widespread premises we want also to be able to safeguard against bad secrets. In the later half of the twentieth century, the concern to prevent "bad secrets" has led to whistleblower protection laws, and the general role of the mass media as the "fourth estate" of government. The difference between what secrets should be punished if revealed versus what secrets should not be kept is difficult to determine, much like the difficulty in determining the difference between disloyalty and dissent. At best, the difference is context-dependent. Any society during times of conflict, such as war, will become more quick to label as "treasonous" behaviors which otherwise would be tolerated.

The awareness of this tension is unusual, perhaps even unique to the U.S. state of affairs. Our laws, and the tension that gives rise to our unusual laws, arise from our experiences in the Revolutionary War. We formed our laws in reaction against, very specifically, the British laws. British law today is widely regarded as among the most strictly controlling of government information in any western country (see Robertson, Public Secrets: A Study in the Development of Government Secrecy). The British Official Secrets Act is far-reaching in its effects[7]. Even before the Official Secrets Act, British treason law was broad and powerful. Based on the idea of lese-majeste, any action which harmed the monarch's person or image was punishable by prison, exile, or revocation of property rights. The British law, in turn, was based largely on Roman law regarding lese-majeste. Roman law would include the selling of information (*any* information about the emperor being given to any other individual, also including any speculation about the emperor, the emperor's health, his actions, etc.), counterfeiting (damages the image because coins were stamped with the emperor's profile), behaving poorly while in a

position that reflected on the emperor (such as being appointed a governor and then absconding with treasury funds, or spending them on ill-advised projects), or of course anything that directly threatened the emperor's person (including the use of black magic).

Roman law is an example of laws which define treason as an act against the government, because the government (the emperor, but before that to a lesser extent the Senate had been protected by a very similar body of laws) was the embodiment of the people. But treason does not have to be defined in terms of actions against the government, and in U.S. law, with our origins based in revolt against a government, there was a preference for basing law on alternative historic traditions. The Greek law defined treason in a very different way, and U.S. law harkens back much more clearly to the Greek conception than to the Roman conception, though the Roman conception became by far the dominant model throughout Europe. The Greek law[8] originated with the concept of "Perduellio," meaning "bad warrior." The obvious case in point is a warrior who either deserts during time of war (which in almost every society is defined as treasonous) or who betrays the army (for example, giving away crucial information, which is what most of the known cases are based upon). The law was then extended to include not just citizens in the military, but all citizens. So "Perduellio" came to include merchants who traded away information that was damaging to the city-state. It also came to include government officials who betrayed their position, and for example the Peloponnesian Wars include a trial of exactly this sort. So treason meant a betrayal *of the people*, or of the *demos* more properly, and might or might not be a betrayal of any particular government. Indeed, the overthrow of the government was quite specifically not considered treasonous. This concept was written into Athenian law, but was refined under the Spartan government into its most widespread form.

Germanic law of the Dark Ages presents yet a third way of understanding treason. Germanic law bears the closest resemblance to the most recent incarnations of U.S. law, in which if an individual has signed an oath to keep government secrets (a necessary signature

before getting a security clearance), then if that individual is found to privately possess duly classified documents then a crime has prima facie been committed. Under Germanic law, the word for "treason" was "trothplight," or more explicitly translated, "oath-breaking." "Allegiance among these early Germans is pervaded with the idea of a contractual relation which is bilateral," notes Lear, p. 130. The feudal system operated on a rigid set of oaths–the knight pledged fealty, but the lord also swore a set of oaths in return. To break that oath, whether lord or knight or peasant, was defined as treason. Yes, the burden of proof for accusing a lord was more difficult, but examples still occurred frequently enough that the procedure was written into the law. The oaths would generally include a phrase that was interpreted as forbidding the sharing of secrets with outsiders, or perhaps even the sharing of any information to an outside party. Similarly, our most recent statutes define as criminal any "possession" or "mishandling" of information which has been properly processed as classified after you have signed the agreement not to reveal said information that is necessary before accepting employment that requires clearance.

Espionage is one element of what would have been treated as treason, which in most other societies is much more broadly defined. The American law regarding treason is limited to acts directly aiding and abetting an enemy during time of war. In some ways this narrow definition has complicated our understanding of espionage. Under this definition, Americans selling secrets to Russia during the Cold War could not be prosecuted as treason. Separate laws, referred to as the "Espionage and Sedition Laws," were passed during World War I, but the battles determining the scope of these laws are still not settled (see e.g. Richard Blum's edited volume Surveillance and Espionage in a Free Society).

In addition to legal questions regarding the boundaries of espionage and sedition law, two other central legal questions arise regarding espionage. One source of contention is the appropriate penalty. In many cases, the prosecution has preferred to settle for a lesser penalty in

return for cooperation in future counter-intelligence efforts. But the threat of the death penalty makes sentencing in other cases a scene for extensive legal and moral wrangling (see for example Elizabeth Bazan's article "Espionage and the Death Penalty"). The third major legal issue regards evidence. The nature of an espionage case is that the central issue is a secret. The prosecution and defense must either argue the case without discussing the central issue, or else the secret must be made open in the courtroom hearing (see e.g. Haydock's article "Some Evidentiary Problems Posed by Atomic Energy Security Requirements" for a review of why various attempts to find a solution are unsatisfactory, see also Newman's article "Control of Information Relating to Atomic Energy" for a prescient view of the problems caused by increasing secrecy). The secrecy also often extends to questions of how the espionage became known. Given that the Constitution (and justice) requires that the accused must know what leads the prosecution to accuse him or her, the secret must either become no longer secret or the prosecution must do without that portion of the case. This evidentiary problem is particularly apparent in cases of technological espionage, especially nuclear.

ELEMENTS OF ESPIONAGE RHETORIC

The history of American espionage law has shaped a legal context in which espionage cases are extraordinarily complex, and the popularity of the espionage genre has created a context in which these complex cases receive more publicity than almost any other kind of criminal trial (with the possible exception of mass murderers and terrorists nowadays). The media context and the legal context are not independent of one another, nor does the media context simply follow the legal trial. Rhetorical shifts in espionage cases can be found to originate in either context, and the two are sufficiently interdependent that a rhetorical shift in one will lead to a shift in the rhetorical strategy employed in other contexts. The legal context, the media coverage, and the fictional genre constraints all interact with the specifics of each individual case. The rhetorical situation that is created by an espionage case requires a

simultaneous assessment and addressing of each of these components. There are certain similarities across particular espionage cases because of the interdependence of these contexts. The similarities create a set of topoi that appear in one form or another in every espionage case.

1. Burden of Proof

The "burden of proof" in rhetorical theory has been used to refer to the "default" setting, where an audience's initial predisposition will or should tend to favor one rhetorical position over another. The term was introduced by Richard Whately in 1828, who intended that the "will" and "ought" of audience's predisposition would be part of their education, and that education he viewed as based on rhetoric. Following Whately, the "burden of proof" means that the rhetorician who is arguing against that initially favored position will have a more difficult case to persuade successfully. The "burden," then, is that additional difficulty that will be faced by those arguing against the status quo (the presumption being that audience's should prefer the known to the unknown) or in defense for a legal case (the presumption being innocent until proven guilty). The burden could only be met by mustering additional evidence, or by demonstrating that the harms of not being persuaded would be greater than other harms faced. These notions have become a core part of the rhetorical tradition, and are taught to debaters and all beginning rhetoricians as their "stock" issues. It is not to be confused with the specifically legal application of the term "burden of proof."

In espionage cases, the burden of proof is complicated by the interdependence of the various contexts, legal and media and genre conventions. On the one side, the government will always be prosecuting, although which part of the government changes at different stages in an espionage case. At the beginning of an espionage case, the government's position will be represented by individuals within the same agency as the accused spy, and those individuals will be responsible for persuading an investigating agency (almost always the FBI) to take up the case. The FBI will carry the burden of representing the government's position to the Justice

Department, the agency which will actually argue the case in court and in public. The rhetor opposing the government in some ways has the more complex burden to analyze, and changes frequently within cases as well as between cases. In the legal setting, the technical burden of proof must be carried by the prosecution, but in the newspaper coverage particularly the rhetorical burden of proof is often on the defense, which will be heard only secondly and only if they have a rhetorical strategy that allows for a narrative form that can break free of the genre conventions and yet remain germane.

This rhetorical burden of proof can be met in a variety of different ways. One way is to privilege one context over the other contexts, and almost always the preferred context will be the legal context. By focusing on the legal context, a rhetor can select strategies that would be ineffective, or even counterproductive, in other contexts. For example, a strategy of challenging the government's procedures such as failure to get warrants or failure to follow proper legal procedures, can sway a judge but will further suggest guilt when presented in the mass media. Another way to address the burden of proof is to muster additional evidence, requiring a wide spectrum of evidence to both challenge the government's evidence and to support an alternative explanation for each of the crucial topos. In other words, the rhetor must address the construction of motivation offered by the government's evidence, their construction of the harms, and their narrative suggesting how the alleged espionage occurred. Mustering sufficient evidence only to challenge the government's evidence, or to address only one of the other topoi, cannot alter the rhetorical situation across all of the interdependent contexts strongly enough to meet the full burden of proof.

But how can anyone prove, "beyond a reasonable doubt" as the specific legal burden of proof demands, that communication occurred when both parties involved deny having communicated? This seemingly paradoxical question is the heart of an espionage case. The burden of proof demands that the investigator and prosecutor find sufficient evidence to prove

not only that communication occurred, but also to prove that which was communicated was a government secret. Considering most of our common definitions of communication within the field, how can this even be possible? Surveys of various definitions can be found at the start of most introductory texts. A review of several (including Trenholm, Miller, West&Turner, Griffin) suggests that most definitions center on the transfer of information or development of shared meaning. Both information and meaning are intangible, so evidence regarding them must link ideas to practices to material results, the only form available to an outsider and presentable in a court of law. The problems with linking the development of shared meaning to material results, and establishing that those links are "beyond a reasonable doubt," is possible only under very particular conditions. The audience must participate in those same "shared meanings" sufficiently that the links formed to material conditions seem obvious. In effect, almost every espionage case is an example of enthymematic reasoning, with the audience itself supplying the necessary premises to enable movement from establishing a believable motivation to believing that it accounts for actions that might result in the evidence presented, i.e. the material conditions that are observable to the audience. Of course, the easiest way to do this, to prove an espionage case, is to have trained observers capture on film or on tape the actual transfer of documents and of money. The desire for this material evidence has led government agencies sometimes to leave spies in place even after suspicions have been raised, risking the compromise of additional secrets in order to secure the strongest case possible. The desire for this kind of material evidence has also led to tensions between government agencies, one more willing to gamble on the compromise of secrets than another, and those tensions add to difficulties already problematic in the intelligence systems of the U.S. government.

2. Motivation

Another way to attempt to prove an espionage case, for the government to meet its burden of proof in the legal context and even more so in the media context, is in establishing

motivation. This question will be addressed at greater length in chapter four, but because this topos is so crucial, some relevant questions must be raised here. What persuades individuals to engage in espionage? The question is of interest in attempting to prevent espionage, and hence the answers that the government believes are built into the safeguards placed on the intelligence system. From the rhetorical perspective, one also needs to consider the answer to that question in terms of what would persuade another audience to believe that an individual would be willing to engage in espionage. In other words, what motivations would we accept to believe that a person would become a traitor? What characteristics lead us to suspect that this is somebody not to be trusted? We need to consider motives both as they are constructed during legal cases and during fictional or biographical writing. Particularly interesting in this regard are the typologies of motives that have been developed by practitioners within the intelligence field.

Questions must be raised regarding the motivation of the rhetors on the opposite side as well. What persuades government agencies to proceed with an espionage case? Or to begin an espionage investigation? One way to answer this question is to turn to the topoi above, and consider again the types of evidence that suggest espionage or the types of motivation believed to lead to treason. But there are costs involved in an espionage case, both opportunity costs (the manpower hours involved are often very high, and there are never as many individuals involved in counterintelligence as in intelligence, so there are always more potential cases than can be pursued), and the costs in weighing the maintaining of secrets vs. potential exposure in court and the blow to the intelligence agency's reputation with the public. There are other motivations that should be considered. It is not coincidence that during the early years of the Cold War there were many more espionage cases than at any other time before Reagan's administration. There are motivations that can be loosely termed "political" in an espionage case. McCarthy-era espionage cases we can see in retrospect were motivated less by evidence and more by the political climate in which prosecuting Communists was a rhetorically effective election strategy.

For example, the American Bar Association during the 70's re-tried the Rosenberg case using the same evidence, and the verdict twice came back "not guilty." Similar reconsiderations of Judith Coplon's case by legal historians conclude that the evidence alone available at that time, if tried in a different court at a different time, might well have led to a different verdict. It seems reasonable to ask whether the striking rise in espionage cases during Reagan's presidency and today during Bush's administration have political motivations as well as evidentiary motivations.

The degree of popular interest in espionage cases suggests that the motivation to condemn traitors is widely shared, and that spies are the archetypal conception of the traitor in America. This may seem obvious, but it is worth considering how it came to be so obvious. American norms were not always such that support for government secrecy and intelligence-collecting regarding other governments would have been a widely accepted rhetorical stance. Clearly not all espionage is created equal; different degrees of harm merit different penalties. We therefore need to consider the "material harms" that motivate the government and presumably the majority of the public to spend rhetorical energy countering espionage.

3. Harms

Because of the American history and the limits of our willingness to apply the label of "treason," an espionage case must include at least some addressing of the topos of "harms." Legally, an espionage charge requires demonstrating that secrets have been passed to an enemy with intent to harm U.S. interests. Three terms in this requirement are worth exploring under the topos of harms: "secrets," "passed to an enemy," and "intent to harm." Each term is contested in legal and media contexts. In general, to establish the harms in an espionage case, only one will be dealt with explicitly, with the other two left implicit.

In attempting to consider the "material harms" of espionage, both for purposes of crafting an espionage case and for refuting espionage charges, government secrecy inevitably becomes an

issue. What are the characteristics of a legitimate "secret?" The government's preferred answer is that documents which are classified are secret. This is particularly an easy argument if the spy has been caught in the act. The argument becomes much more difficult if the espionage must be established based on a foreign government doing or manufacturing something. Consider an example: the Germans intercept a shipment to England containing some weapons during World War I. Did the Germans know to intercept that particular shipment because of espionage? Did they perhaps just get lucky, stopping a random shipment, or had they been told? If we consider as secret only documents that are classified, were all of the documents related to the shipment properly classified, including the bills of sale from the manufacturer as well as the bill of lading, and any other orders related to the labor performed? The same questions become particularly poignant in relation to scientific espionage. To establish that information was "secret" requires that it not have been available anywhere in the open literature, and that we can prove the enemy did not develop that information through research in the same way that we ourselves presumably developed the knowledge. In each of these cases, the government's definition of a legitimate secret is that which the government has classified.

But what are the proper limits on government's limitation of communication? There are harms involved in espionage other than simply the loss of secrets, if government's ability to control communication is not itself limited. Specifically, what ought to be considered properly secret, and hence treasonous to communicate regarding? This is a crucial question in all espionage cases, even when it is not addressed explicitly. If the government either had no right to consider the material secret, then espionage is a difficult case to make. The majority of courts have been willing to accept the classification standard, but it is not unprecedented to require that the government establish that the classification was reasonable. The clearest example of such a case is the Pentagon Papers case, though no ruling was made to set precedent for later cases. Arguments over the legitimacy of secrets are predicated on an additional underlying,

unanswerable question: How can we reconcile the tension between secrecy and classification versus freedom of speech and responsible democracy? There are ethical questions, but there are also questions of efficacy. This ties to the final question posed here, because security can be achieved either through superiority (and in terms of technology at least that might be best achieved through open exchange among scientists) or through secrecy (maybe).

Establishing the harms of espionage also requires that the recipient of the secrets should not have those secrets. America's unique history with treason and espionage meant that for most of the country's existence espionage could only occur during times of war, when the U.S. had declared enemies. Today this is the element of espionage cases that is most rapidly changing, subject to rhetorical pressures in many contexts. The notion of an "enemy," in an international environment of rapidly shifting alliances that form and shatter depending upon the issue under discussion, makes the rhetorical strategy unstable. As the CIA's George Tenet[9] has pointed out, an enemy today can become an ally tomorrow, and any country could become an enemy under different circumstances or as we learn more. In the legal context, espionage charges have been brought in cases of sharing classified information with an ally, accepted in a plea-bargain in the U.S. vs. Pollard case. Today we could also consider a rhetorical situation in which secrets were not successfully passed, but where the characteristic strategies of espionage arguments are deployed as in any other espionage case. Brian Regan was accused and convicted for "attempted espionage," having offered to sell secrets to the highest bidder among twelve countries that are considered enemies of the U.S. Clearly this stretches our understanding of espionage rhetoric in a slightly different direction. No secrets were sold, but does that mean espionage did not occur?

The Regan case works because the rhetors representing the government can emphasize the harms by highlighting both the dangers of selling clear secrets to unstable enemies, and also by emphasizing the intentionality. The deliberateness with which the bids were solicited speaks

of significant effort over several years. But as communication scholars, we are intimately familiar with the difficulty of establishing intentionality. Regan's counter-argument is that while the communication was intentional, the intention was to learn about the intelligence operations in each of these countries, to enhance national security rather than harm national security. The question of intent relates to harms in scientific espionage in a particularly unique way: a scientist who is questioned cleverly, such that he does not recognize he has communicated secret information, can be accused of mishandling classified information but cannot be accused of espionage. Establishing intention to harm ties back to the topoi of motivation.

4. Texts and Relations Between Texts

There are additional characteristics of espionage rhetoric that can be noted in almost all espionage discourses. One such characteristic element is the notion of borrowed credibility, called "status conferral" by Robert K. Merton. A persuasive text appearing in the New York Times will have a different ethos than a text in the Edwardsville KS Monitor. This becomes even more crucially true when the interdependent contexts of espionage rhetoric influence one another. There are also numerous rhetors representing both sides of any given espionage case, and the ethos of each individual rhetor will contribute to the perception of the texts produced by other individual rhetors supporting the same position. The credibility of one text influences the credibility of each related text. The constraints imposed on each text by the specific situation it addresses also influence related texts. Each medium imposes its own set of constraints: espionage texts produced for television must meet different constraints than those produced for newspapers. Visual media rely on a set of conventions to convey harms, for example, that include darker lighting and ominous music to establish the seriousness of the treason occurring. Newspapers must also convey the severity of harms, and they tend to rely on repetition of key phrases and enthymematic reasoning to do so. Different contexts also impose different constraints, so that the needs of media coverage for clear plotline and character development in

turn influence legal rhetoric. The constraints on legal rhetoric, such as emphasizing rights and procedures, in turn influence espionage rhetoric in other contexts, including the historical/fictional genre. The historical/fictional genre provides the dominant resource for understanding the constraints on narrative that influence both newspaper and visual media coverage.

There are significant differences between newspaper coverage of real-world espionage cases and fictional accounts of espionage. But the similarities are more striking than the differences. This becomes particularly important to consider when asking questions about why or how espionage occurs, because fictional accounts provide answers that become formulas. The primary topoi of espionage texts are all shaped by audience expectations, which are largely derived from historical/fictional texts. I refer throughout to this genre as historical/fictional texts, because of the premium on conventions that provide the simulation of reality in fictional texts, and because as historians have pointed out in recent years, histories are always also fictions, in the sense of being narrative constructions.

5. Communication about Communications/Definitions

Strikingly, one of the possible argumentative topics that seldom comes up in espionage rhetoric is consideration of the secrets themselves that are being communicated. In part this is because secrets are more interesting when they are maintained as secrets. Sissela Bok introduces her philosophical exploration of the ethics of secrecy with this observation. "Secrets, once revealed, will seem paltry and out of proportion to all that went into guarding them." (p. 5) Secrets are rhetorically effective only while they are unknown, and the very etymology of the word carries some suggestion of this: "secret" comes from the same word from which we derive "sacred," both based on a word that meant "set apart." (Bok, pp. 6-9) The secret forms a kernel of the discourse that is conspicuous by its absence. Assumptions about the nature of secrets are evoked through the use of words like "national security" or descriptions like "personal privacy."

We talk around the secret, a kind of meta-communication about a kind of communication that is taboo, forbidden, illicit. What kind of communication is defined as illegal, and on the basis of what criteria? In other words, what gets classified and why? The short answer to the question of what gets classified is a document produced by the State Department listing militarily-relevant technologies and dual-use technologies--short in this case meaning some 30 pages in summary. The full list is longer than the Manhattan yellow pages, according to military sources with access to the full classified document. Questions of how this list is devised will not be addressed in this project. It is interesting, however, to note here that the State Department has responsibility rather than DOE or DOD. Control of secrets–of defining what counts as "secret" in this case–is a form of power, just as control of any knowledge is power.

The list of classified topics is restricted to technologies, but for this purpose "technology" is defined very broadly, including various types of procedures or techniques, and including knowledge of certain structures as well as the material arrangements that we traditionally think of as technologies. These technologies are forms of knowledge that exist in a material form, exist in numerous documents, exist in various forms in the minds of few or many. The classification limits documents, but what does it mean to classify the contents of an individual's mind? The material form of the technology is also often problematic for controlling and keeping secret. Knowledge that cannot be used provides no advantage, but we cannot both keep knowledge secret and put it to use. President Bush is forced to reveal the knowledge gathered through secretly tapping Iraq's communications if he wants to persuade others to believe his claims of weapons of mass destruction. When we actually use the new top-secret unmanned spy plane, it is not controllable in the same way that documents are–it can get shot down and captured by the very enemy it was developed to give a secret edge over, it can be spotted by the secret spy-satellite of another country. What does it mean to think of knowledge, especially scientific knowledge, as proprietary, a form of property that can be possessed, and defended if

needed by keeping it secret?

6. Typology of Cases

To understand the rhetorical strategies and challenges in a particular espionage case, it is necessary to analyze the type of case it has been defined as. Just as different situations call forth different types of epideictic rhetoric, and the types cannot be produced or evaluated without analysis of the unique and specific context, so also with espionage rhetoric. There are several possible ways to classify different types of espionage rhetoric, and the variations within those different schemes of classification are as many and varied as there are possible espionage cases. What types of illegal communication occur? One way to analyze differences among types of espionage cases is to consider the different types of information that are being communicated, which relates closely to the topos of harms. Given that the secrets being communicated might not be available for analysis directly, the easiest way to understand the difference is in the government agency that is being betrayed. Another useful insight that can be gained by considering the agency in question is that it will explain something of how the espionage could have occurred, and potentially something of why (relating to the topos of motivation). The agency whose secrets are being compromised will influence much of how the case develops, since the first persuasion is almost always internal within the agency, and since the organizational structure and function shapes the rhetorical goals of the government rhetors during the early stages that set the rhetorical situation for the entire case. So, for example, an espionage case that begins in the DOD will be more likely to get prosecuted but will also more likely involve only internal audiences than a case that originates in the CIA. The easiest contrast to see is in the difference between DOE cases compared to any other agency. The introduction of the possibility of nuclear espionage creates a rhetorical shift that impacts every rhetorical context.

A second classification schema that is useful in analyzing espionage rhetoric is the

question of how the espionage is discovered. In principle, espionage cases could begin with the introduction of any new piece of knowledge that creates suspicion in any individual working in counterintelligence, even informally. In practice, by contrast, the beginnings of espionage cases occur in only a small, limited number of ways: they are discovered when the spy is betrayed in turn, when the recipients of the secret knowledge alters their behavior in a way that can be interpreted as a sign of having received illicit communication, or when the spy's own behavior is interpreted as a sign for suspicion. The possibilities parallel the extrinsic forms of proof enumerated by Whately: testimony, signs proving cause/effect, and direct observation. Analyzing espionage rhetoric according to a "mode of discovery" schema is particularly useful for a rhetorician, for this guides the first two canons of the initial rhetoric on both sides in each particular case: invention and arrangement. The mode of discovery is only rarely a topic that is explicitly drawn upon in any rhetorical context other than internal to the agency of origination. The exception is the historical/fictional genre, where a convention exists that is sometimes drawn upon of alternately narrating events from the point of view of the spy and the principal investigator, in which case the mode of discovery will be important for narrating the pursuit the investigator leads.

A third classification scheme that might be used for rhetorical analysis of espionage cases is to consider the traditional sender-channel-receiver triad. There are some interesting rhetorical constraints based on receiver, because the question who is receiving the secret communication is directly linked to establishing the harms of the betrayal. The only cases likely to appear in a media context or in a historical/fictional context are those in which the recipient is China, Russia, or today an "axis of evil" nation. But a survey of the all the government's espionage cases would reveal that nations such as Cuba, Israel, Nicaragua, and Mexico are often the receiver of the illicit communication. If we were to broaden our consideration to include corporate espionage as well, France and Japan would almost certainly lead the list as largest

recipients of secrets. The channel for transmission of the illicit communication is an issue in virtually all rhetorical contexts, and a classification scheme would be useful in considering the constraints on the original rhetors involved (the spy himself/herself and the receiver). One channel would be technologies of various types, such as encrypted computer messages today, or previously cipher machines such as Enigma or coded static on a radio wave. Another channel would be clandestine meetings–the importance of face-to-face communication is nowhere more clearly demonstrated than the risks spies and their agents will accept for the advantages of such communication, given that this channel is easier to detect and easier to prove later than any other channel. Other possibilities are as varied as spies are creative: arbitrary signs such as chalk marks in selected places, color-coded clothing or light flashes, significantly mangled trash, to name just a few sign-systems that have been used in the history of U.S. espionage.

7. Impact

A final consideration in analyzing an example of espionage rhetoric is that the strategies drawn on in espionage cases are not isolated from rhetoric related to other topics. The privileging of secrecy in espionage rhetoric cannot help but influence how secrets get talked about in other situations. What impact does espionage have? The popular interest in discourses that deal in layers of secrecy and layers of betrayal, in which questions of trust and distrust become central and finally unanswerable except in the negative, creates a rhetorical situation that encourages paranoia. Conspiracy theories and espionage rhetoric combine and form a self-reinforcing cycle, and both force audiences to make a "leap of faith" to trust or distrust government, because knowledge cannot be relied on to guide us. What effect does the secrecy that is a necessary precursor to espionage have? On the governments involved? On the publics made aware through various textual accounts of espionage? On the individuals engaged not only in espionage but also in other areas of secrecy? Much has been said about the harmful effects of secrecy on scientific research (see e.g. Society 1986, or 1990 Committee on Science, Space &

Technology). Communication scholars also tend to take for granted the harmful effects of secrecy, but perhaps some of those assumptions should be made explicit. In my concluding chapter, I will consider some of these impacts in greater detail, drawing on the espionage cases considered in the following three chapters and also on additional studies.

PLAN OF PROJECT

The following chapters will focus on three recent examples of espionage discourses. They will focus particularly on the discourses surrounding three specific spies, organized with the figure of the spy as the central focus. "The identities of traitors are a reflection of the political and social contexts in which they live and function," (p. 311) as Ben-Yahuda points out, and thus biographical accounts of spies are a particularly key site for rhetoric. Two intertwining themes should emerge from studying these three cases: 1) trust and 2) evidence. These themes are always integrally related in espionage cases. There are also two "big" questions that emerge. One question is about the organizational structures that create these espionage cases, the ways in which they both enable and constrain espionage. Looking at organizational structures is useful for understanding why things happen the way they do. The weakness of organizational analysis is that rarely does it illuminate the uniqueness of a particular case. It can never answer the question of why this person spied but another person in the same organizational context did not spy, or why one spy was caught and prosecuted but another spy was not. The other question is about the ways in which we talk about espionage cases, including the various rhetorical strategies used by all of the parties who have a case to make, either explicitly or implicitly. Analyzing the rhetorical strategies should illuminate the specific mechanisms of the particular cases, but in addition it should also integrate our understanding of espionage cases into the broader fabric of American society by showing the ways in which espionage rhetoric takes from and contributes to other forms of public argumentation.

Under the topic of understanding the organizational structures that are the context for

espionage cases, we are trying to look for the mechanisms of constraint and resources of enabling. That necessitates considering the immediate context for each espionage case, which is of course also necessary for analyzing the rhetoric that emerges. The immediate context for each case will be part of the chapter, rather than part of the introduction. But more generally, actually understanding that context, I will argue, requires looking at not just the immediate context, but at the larger structures: the legal structure, the governmental structure, the bureaucratic structures, and the boundary-work that preserves the relevant structures. To understand, for example, the legal structure that shapes espionage cases, we need to understand something of what the current structure is, how it came into existence in that form. This means we might recognize that alternatives exist and that they continue to serve as resources that can be drawn upon rhetorically. For understanding the governmental structures that relate to espionage, one must understand the functions that intelligence agencies perform and their relation to other governmental structures that constrain and enable them, and that influence what remains stable and what can change under which pressures. And to understand the bureaucratic structures that shape espionage cases, it is not enough to know the name and hierarchy within the bureaucracy, one must also understand something of the history of the bureaucracy because that history is the source of the resources and constraints within the bureaucracy. These organizations developed into the current form for a reason, and consideration of that reason tells us much about why the organizations react as they do: why they ignore, or conceal, or exile, or persecute, or use a spy. And by understanding that alternatives exist for every organizational structure, one might be able to see alternatives to how espionage cases develop, and thereby better analyze them.

Under the topic of analyzing rhetorical strategies, we are also trying to look for constraints and resources, but also at opposing arguments. Students of rhetoric traditionally have tended to focus on single rhetors and even singular texts. Espionage cases are difficult to analyze that way. It's not just that rhetoric in general cannot be analyzed without understanding

its context, though that is also true. The challenge with espionage rhetoric is that the true significance of the argument strategies that get used is only apparent when we look at collections of rhetors (say, all of those rhetors arguing in favor of an alleged spy) or even better a collection of several collections of rhetors across a number of different cases. One of the difficulties in analyzing rhetoric in organizational contexts is that it's also sometimes difficult to distinguish the individual or group responsible for a given text, and so identifying the rhetors and the discourses that "belong" as part of an analysis becomes exponentially more difficult. The same difficulty arises with audiences for organizational rhetoric. My solution has been to sidestep many of these questions that are traditionally so central to rhetorical criticism as being genuinely unproductive here. The use of rhetorical theory to understand espionage cases provides insight about the role of evidence and the ways in which we negotiate the role of the traitor among us. The study of espionage cases can also contribute usefully to rhetorical theory, because of the unusual emphasis on silence and secrecy as integral parts of rhetoric, and the unusually explicit discussions about trust, the underlying basis of persuasion.

Chapter 2, Aldrich Ames

This chapter aims to focus on the institutional structures bearing on espionage cases, and the delicate balance of trust and distrust that an intelligence agency must continuously renegotiate. The Ames case is particularly useful for considering the differences between institutional positions, and the interactions among them, because Ames' case continued for so many years and involved many individuals and organizations.

Chapter 3, Wen Ho Lee

This chapter aims to focus on the interactions among texts as they appear in a variety of different mediated contexts. The

rhetoric involved in a spy case does not occur in isolation, as it is impacted by numerous discourses that range from those directly related (rebutting the original rhetor's position, for example) to those more distantly related but still influencing the text's reception (for example, a part of the rhetorical history that forms constraints).

Chapter 4, Robert Hanssen

This chapter focuses on the ways in which the identity of a spy gets constructed. The chapter will approach this question in two ways, first considering the ways in which the spy's identity gets constructed during the investigation. This is largely a process that is internal to the institutions but which gets rationalized during later discourses. Secondly, the chapter will consider the ways in which the spy's identity is understood in the broader context of a society that is forced to grapple with questions of trust and secrecy. Questions of identity in espionage cases revolve around constructions of motivation. The rationalizing of the spy's motivation and attributions of motivation are the primary focus of rhetorical analysis in this chapter.

A Note on Reading Strategy

A caveat is in order before proceeding. Espionage involves questions of treason and loyalty, trust and betrayal, secrecy and disclosure, and truth and falsity. These sets of antitheses that are invoked by the use of the term "espionage" are all emotionally loaded terms. Espionage itself, however, needs to be maintained as a neutral term, at least for the purposes of this study. Espionage is a practice engaged in by nearly every nation. The U.S. invests billions of dollars each year in committing espionage, and in attempting to prevent other countries from practicing espionage against it. As scholars, it is vital that we not treat "our" practice of espionage any differently than "their" espionage. Sociology of science benefitted immensely from the recognition that treating success and failure in the same terms, to be explained via the same

mechanisms, led to clearer understanding. In the same way, for the sake of achieving a clearer understanding of espionage, it is vital to bracket the question of "which side" is benefitting from a given instance of espionage, difficult though that may be.

"Never attribute to conspiracy what can be more simply explained by human stupidity" (an adaptation of Ockham's razor, provided on the witness stand in the Lee trial by John Richter, nuclear physicist-cum intelligence analyst-cum defense witness)

Aldrich Ames and the Conspiratorial World of Espionage

Aldrich Ames is generally considered the most damaging spy in the history of the CIA.[10] Evidence of his importance can be seen in the number of newspaper articles devoted to his case (330 articles), and the fact that the Russians valued him enough to pay him more than any other spy in U.S. history: three million dollars, with the promise of more when/if he escaped to Russia. Ames' information allowed the Russians to close down at least 100 intelligence operations. Even worse, at least ten (more likely seventeen) U.S. and allied agents were executed when Ames betrayed them to the Russians, according to the Defense Security Service's summary of the case. During a spying career that spanned almost ten years, Ames sold to the Russians documents compromising not only U.S. intelligence activities, but also the intelligence activities of our allies when they shared information with us[11]. For his efforts, Ames received three million dollars from the Russians, and a lifetime prison sentence from the Americans. The prosecutors had initially argued for the death penalty for Aldrich Ames and a lifetime prison sentence for his wife Rosario for her role of giving advice and providing cover. If ever there were a clear-cut case of criminal espionage, Ames is almost certainly that paradigmatic case. In the Ames case, clearly we should see secrecy as a virtue rather than a vice, a case where Habermas' ideal of open communication is damaged and damaging (even damning) for society as a whole. Ames' communications led to several deaths, a particularly cruel death given Russians' reputed treatment of Russian citizens caught spying for the enemy. Additionally, his

spying damaged our intelligence agencies' ability to do their jobs, cost us the trust and cooperation of allied intelligence agencies, and wasted both the time and money the U.S. had committed.

OPENNESS AND SECRECY

Or is this easy condemnation really that simple? Certainly Ames' own view is that he did not in fact betray his country. He had initially entered a "not guilty" plea when first brought to trial, on the basis that the espionage law requires establishing "material harms" to national interests, and he argued then and continues to maintain today that the harms to national security were not sufficiently significant. Even after the plea-bargain in which he promised cooperation with the damage assessment, Ames has argued in both the legal milieu and during internal debriefings that the communication in which he engaged has not hurt U.S. interests. "I didn't feel I was betraying my country. ...It's [intelligence work] a nasty kind of circle, with terrible human costs... and maybe a very few political implications, but not much more."

Ames' perception of the futility of intelligence, and even more so of counterintelligence, is not unique to Ames. In transcripts of interviews between Ames and his debriefers in the CIA, there is a cynicism shared between the CIA interviewer and Ames about the use of intelligence. The shared cynicism can be seen through nonverbal means such as numerous conversational overlaps, through verbal signs such as both using terms like "frustration" frequently, and in the ways conversational moves echo each other. Communication scholars label this phenomenon "entrainment," and note that it usually occurs where there is both similarity and liking. So, even though Ames has been more eloquent and outspoken regarding the flaws in the intelligence system than any other spy or most other former agents, still it can be seen that his views are not really atypical. Two other recent books, by FBI and CIA former agents, testify to similar recognition of the limits and problems of intelligence agencies, though the emphasis apparent in those books focuses more on the revelation about crimes committed by informants which were

concealed by the agencies in question.

With that caveat in mind, consider the following arguments Ames raised in a recent (February 2003) interview with CNN.

> "The human spy, in terms of the American espionage effort, had never been terribly pertinent. It was not a matter of a relative ascendancy and a relative decline."
>
> "... I found that, for example... our Soviet espionage efforts had virtually never, or had very seldom, produced any worthwhile political or economic intelligence on the Soviet Union; that what we had, what we acquired through espionage in, we did a little better on some technical... on some weapons and defense things, but these were spotty, these were fortuitous: Tolkachev, who came and insisted on giving us material despite our initial fears;... that our espionage efforts simply were not productive, except in one area - as a strange set of circumstances, in the counterintelligence area they were extremely successful for a variety of reasons."
>
> "Everything that one of these sources produced, of course they were closely held because they were so sensitive, but in speaking with analysts later who worked in the area of Soviet foreign policy, none of this made it into intelligence production, no matter how closely held, that seemed to me to result in any better understanding or a better... in any... that they were useful to policy-makers in any particular way. In fact, what they did was, they undercut the bases of American policy, both of these sources, demonstrated... to the extent that their materials could support it, demonstrated a rather *ad hoc* defensive approach from Gromyko and Brezhnev and the Soviet foreign policy establishment at the time, improvising, *ad hoc*, or worrying, defensive, not the secret master plan for world conquest that was so much at issue in the late Seventies, when many people, including policy-makers, took the view that the West was under a new coordinated aggressive assault, and these materials ten... just simply not only didn't support it, but tended to contradict it."

In other words, Ames is saying in this section that the disclosure of the secrets he sold did not impact our national security, because the intelligence that was being collected from these sources was not having any impact on U.S. policy or actions. The reasons Ames speculates regarding why the intelligence had no impact on U.S. decision-making we might easily dispute. It is difficult to dispute, in hindsight, that Ames' assessment about what intelligence impacted U.S. decision-making seems to be correct. The segment of the intelligence community which had

predicted the downfall of the Soviet Union did not impact policy to the same extent that the segment of the intelligence community sounding alarms about the power of the Russians. Ames himself has a variety of hypotheses as to why intelligence does not impact U.S. decision-making, and hence fails to impact national security. We could perhaps suggest additional possibilities, as Ames's debriefer does. Ames responds:

> "But, you know, it's not entirely a matter... what you mentioned before is very interesting, because the resistance of policy-makers to intelligence is not just founded on an ideological presupposition - in other words, that the Soviets must be viewed as aggressive, or the Americans must be viewed as aggressive; there's strong complements of that on both sides, but the other real-world factor, and not having too much to do with ideology, is that senior policy-makers - prime ministers, presidents, foreign secretaries and the like - operate in a regime of so many constraints, budgetary, political diplomatic, that their room to develop and initiate and implement policy initiatives based on the best intelligence view is extremely limited and in fact they tend, by the nature of things... senior policy officials... to distrust intelligence sources and intelligence officials, not because of a long record of failures or anything like that, although that can at any given time have an effect, but simply that these people don't understand what the real problems are and how we have to work to get our policy laws. So there's a built-in problem with institutionalized, bureaucratized, highly developed systems of collecting and producing intelligence for policy-makers. Now Great Britain in a sense pioneered the idea of a workable system for getting this cranked in, but I think it's remained a slightly more flexible system than the approach taken over the years by the CIA, which has become a vast institutionalized machine that cranks material out endlessly and is very easy for senior policy-makers to ignore - or, let's put it this way, to scan, to read and say, 'Well, that's all very well but of course we can't do that.'"

Regardless of the reason why intelligence has no impact on policy, even on those occasions where the intelligence community is in relatively complete consensus as to the validity of the source of the information, the result is that in light of the disconnect between input and output, there is less motivation for secrecy to be preserved. In light of the value placed on freedom of expression in U.S. ideology from the moment a student enters school, pressures towards openness are likely to reassert themselves.

> "...[I] had come to the conclusion that the loss of these sources to the United States Government, or to the West as well, would not compromise significant national defense, political, diplomatic interests, as I saw them. This calculation - or this belief, perhaps is better put - this belief grew out of my experiences in my profession, in my political outlook on the world, my own assessment of where things stood between the Soviet Union and the West. And I would say that this belief of the non-injurious nature of what I was doing... this belief was not a calculation that I made that then enabled... that then justified my turning the names over. Rather, it was a kind of a precondition, that having this belief then allowed or permitted me to do what I did for much more personal reasons. Had I not had that conviction or that belief, that strong belief that this was harmless apart from sort of institutional bureaucratic interests - had I not had that belief, I don't know that I could have done what I did."

> "For reasons that I considered sufficient to myself, I gave up the names of some of the same people who had earlier given up others. It's a nasty kind of circle, with terrible human costs... and maybe a few political implications, but not much more."

> "Leaving the realm of names I did provide quite a lot of short- to middle-level foreign policy and national security policy information, and this is something that of course the press... I mean, names are all that counts... this is something that not only the press, but government debriefers, in debriefing me about these things, have very little interest; no one's interested really in knowing what policies or what... you know, what diplomatic initiatives or arms negotiations might have been compromised by me. These are areas that they have just briefly touched on; nobody's very interested in this."

In the quotes above, we see Ames reflecting on his role as traitor, as spy. The crime for which he is best known is the betrayal of the names of our sources inside Russia, which led to their deaths in most cases. Yet from within Ames' perspective inside counterintelligence, he sees himself as dealing in a kind of poetic justice: those who betrayed, are themselves betrayed in turn. He correctly notes that nobody is very interested in any secrets he sold other than the names of our sources and agents. The question of what impact those secrets have on national security never comes up, amidst the furor over the seventeen names. Below, we see the agent running this interview speculating as to why this reaction:

> "Do you think that we throw our hands up in horror and reach for the smelling salts because we don't really know how nasty in a way - and I'm not trying to be offensive about intelligence as a whole, but don't know how nasty some bits of it can be, and that the ones who actually live with the nastiness of it, and the betrayals and the deaths that are entailed with that, are used to something and are inured to it, so that the taboo may be very slightly less, and that the general public is as horrified as if we were to walk into an abattoir in a way and say, "We'll eat the steak but we don't want to watch the beasts getting killed," and that we are in effect paying people like you and Polyakov to do things we don't want to do ourselves, and that therefore it's a common language and a common way of behaving?"

Ames responds at length, over the course of several further conversation turns during which both parties speculate further about the outcome of the espionage case:

> "The proposition that espionage corrupts the people who practice it, or at least corrupts the people who recruit, induce or handle the spies who are betraying their trusts, has a... has a lot of weight to it. I think it is corrupting; it is corrupting for men and women to.. induce and to pander the kinds of betrayals and personal tragedies that result from these betrayals. In any open-eyed view of things, it is corrupting to engage in such activities: corrupting to the person who does it, it's corrupting to the... to the people or institutions who sponsor it. This is why espionage has never been respectable; this is why espionage has always been disreputable, because people instinctively understand it. You know, I don't think the films of James Bond and romantic views of spies have done anything to alter the public revulsion to what espionage really is, any more than you know, people, despite law-and-order, tough-on-crime views are likely to really like the public hangman. that stench is there. And it's deeply compromising to the people in institutions that practice it.

> "I suppose that my case, if it were to exemplify anything about the Cold War, simply exemplifies the meaningless [sic] of espionage and of intelligence generally, to a considerable extent, to the history of the Cold War, to the great events that moved nations and people. That it shows in pretty high relief a lot of the personal tragedies and sufferings that are a consequence of espionage, the moral insensitivities, the moral and ethical insensitivities, the calluses that grow up. A pretty good illustration of all of that."

> "Well, let's put it this way: it's an esoteric profession, like being a priest, or a military man, or a cop. These are all... you know, all... many professions, almost every human endeavor, has, or perceives itself to have, a special esoteric significance; and of course, espionage is one of those world-class systems of

> esoteric, of self-designated specialness, uniqueness, dedication, purpose and mission. And the secrecy isn't so much a genuinely independent factor, but it's a marvelously invigorating, aggravating factor, and so any espionage service is going to have a tremendous amount of inwardness and secretiveness and all of that. This goes along, and then you have to put it in mind of the kind of corrupting effects it has. this is why espionage services, in my view... Espionage services should really be kept somewhat as the SIS has: small and weak, in bureaucratic institutional terms. The CIA and the KGB are espionage services, the First Chief Directorate and some others, and then the.. CIA's became institutionally large and powerful, and largely self-empowering after a certain point. This is a very bad situation. They should be kept small and weak and powerless. In this way, they would be used only for those things that cannot be otherwise done, are so valuable the risks are worth it. Otherwise you have a hypertrophied sort of institutional monster, and... not staffed by monsters, but the organization itself. And the esoteric, inward-looking nature of the profession is one that doesn't take very well to being bureaucratically expanded."

Ames brings to our attention the dangers he sees as inherently involved in intelligence work. It is possible to argue that Ames is wrong, and his own biased interests might be give additional weight to such an argument. Even if we accept that Ames' arguments are valid, however, the solution he proposes, of keeping intelligence agencies small, is counter to the reality. Since World War II the American intelligence agencies have experienced continuous growth, a trend unlikely to change in the post-9/11 environment. And while intelligence agencies increase, it is in all probability inevitable that double-agents will continue, and it might be more productive to turn our attention at this point to studying how such cases arise.

THE SPY AS FOOL

Ames's case has been the subject of four full-length books, of many media articles, and of no less than three Congressional hearings and/or reports. My goal here is to explore the ramifications of Ames' case for its relevance in terms of communication, not recount extensively the factual events that have been covered in other forums[12]. Ames' case is important for communication scholars because it reveals an unusual shift in the usual tension between openness vs. secrecy, and how each relates to establishing trust and credibility. Communication

scholars frequently equate open communication with trustworthiness, and "secrecy" gets treated as something of a devil-term. Perhaps that is inevitable for communication scholars, given our field of study. But the presumption that secrecy is untrustworthy and openness inspires trust is a set of equations that are arguably held true as the default setting in "common sense," as well. Sisella Bok, in her books "Lying" and "Secrets," must go to great lengths to find examples of cases where common-sense-ethics favor either of those two things. Honesty has been considered the bedrock virtue, both in philosophy (Kant's Categorical Imperative) and in civic life. If the primary directive of medicine is "first, do no harm," then in civic life the primary directive could be first, tell no outright lies, and secondarily, omit no crucial truths. National Security has traditionally been one of the few loopholes allowed in the commandment of openness and honesty. The Ames case provides the most vivid example in recent history of why openness in National Security is not necessarily a virtue, and why lying and secrecy in support of National Security is not necessarily a vice.

Ames describes his ideological disillusionment as a precursor, a necessary precondition before espionage could be considered. He attributes the immediate impetus to his sense of desperation resulting from debt and a new wife with expensive tastes. The stories usually told about Ames revolve around his greed. But this is an oversimplification. Ames' motivation apparently was based on a desire for both money and for revenge against his employers for not treating him well enough. Ames was a career intelligence officer. His father had worked in the CIA, and Aldrich Ames began working for the CIA before finishing college. Ames had flunked out of college on his first attempt, at the University of Chicago. He later returned to Georgetown University and finished a bachelor's degree in history.

Ames should never have been a CIA agent. His father's service record with the agency seems to have served to vouchsafe his initial clearance. In most other organizations, such nepotism would be frowned upon. Other intelligence organizations have also had periods in

their organizational histories when nepotism was common–Los Alamos National Lab, for example, is the subject of numerous jokes related to the frequency of relatives hiring relatives. Ames was hired in spite of the fact that every available bit of evidence even then suggested he was unfit to serve. He drank too much, he had flunked out of college, and he had difficulty making friends. Difficulty making friends may seem like an argument that should not matter when hiring, but given that the job of a field agent for an intelligence organization is to recruit agents, that should serve as a warning sign that perhaps an individual would be better off serving elsewhere. Difficulty making friends should also serve as a warning sign indicating higher probability of espionage, given that individuals who don't fit in are less likely to feel loyalty to the system (consider Hanssen's case for example). As soon as Ames began working in the CIA, the warning signs were plentiful. Foremost among those was his continued drinking with the resultant problems, such as losing his driver's license due to drunk driving and forgetting his badge in the bar. Ames failed to receive any promotions because of his inability to recruit a single agent, though he successfully "handled" two while working in New York, before those agents were rendered inoperative. Ames' two agents were lost because a book (Legend: The Secret World of Lee Harvey Oswald, by Edward Jay Epstein) named them. Many within the CIA believe that Angleton had been the source for the book's author. James Jesus Angleton, then head of counterintelligence at the CIA, had suspected that TOPHAT and FEDORA (the codenames for the agents) were double-agents, and presumably he revealed their identity publicly because he was attempting to blow their cover.

In addition to failing to recruit while in New York, Ames was reprimanded for blunders in the most important case he ever handled: he simply forgot his briefcase full of photographs taken from FEDORA, the Russian spy he was handling. The briefcase was left on the subway. It was fortunately returned by the woman who had picked it up, when she realized what was inside and immediately contacted the FBI. Ames' other important case that he handled was that

of Vitaly Yurchenko, a Russian defector who later re-defected with much press coverage of his story that the CIA had forcibly kidnaped him. Today there is still debate as to whether Yurchenko had ever been a genuine defector, or whether he was a plant to divert attention away from the new information source the KGB had (Ames) and the large number of assets (intelligence jargon dehumanizing the individuals who sell secrets to us while continuing to work in Russia) being executed as a result. Ames also did not receive promotions because he refused to accept overseas assignments for several years, preferring to stay in New York with his first wife, Nancy. After Ames was finally pressured into serving overseas as supposedly every CIA agent must, Ames was sent to Mexico City after he refused to travel to Russia or Africa. In Mexico City Ames' drinking was a continuous problem, and he became more focused on courting the Colombian Cultural Attache, Maria del Rosario Casas Dupuy. Ames' dissatisfaction with and constant complaining about his career combined with his drinking led to poor performance reviews, in the bottom 25% for agents that went through training at the same time he did. One would think that suspicion would have been raised by Ames marrying Rosario, who was known to have previously worked in intelligence. The position of Cultural Attache is a position that intelligence agencies often use as cover for an intelligence agent. Rosario seems not to have been an intelligence agent in Colombia, which is perhaps why she had been easily and eagerly recruited as an American intelligence asset (and had been approached by the Russians) before she met Aldrich Ames. The position itself, however, is generally viewed as a cause for suspicion. Another missed signal was a sudden influx of brazenly displayed wealth– driving a Jaguar while abroad and then buying a new one upon returning to the US, paying cash for his half-million-dollar house rather than getting a mortgage, all supposedly because his wife's family was wealthy? Notice here an interesting parallel to the claim that we will see in the Hanssen case: family wealth that cannot be easily traced because it was either from outside the U.S. or in the form of non-liquid assets. With so many signals suggesting an individual

willingly engaged in espionage, suspicions should have been raised much sooner.

To be fair, there were suspicions raised long before his 1994 arrest. Part of his unhappiness with his career was caused by those suspicions. Ames was not promoted as quickly as expected (meaning not as quickly as he felt he deserved, but also not as quickly as others who began training at the same time as he did), and his performance reviews continuously included criticisms of his problems with alcohol. Eventually, it became clear that he was a failure at field-work altogether, so he was brought back to Washington D.C.–and put in charge of Soviet counterintelligence.

Why counterintelligence? Because at that time, during the late 70's and up until mid-80's, counterintelligence was a backwater, a disorganized hodge-podge of individuals who did not fit in anywhere within the CIA's culture, including almost all of the women who worked in intelligence, a few old-timers still employed from the days of World War II, and other misfits. A variety of factors combined to turn counterintelligence into the backwater of the agency. One of the powerful forces discrediting counterintelligence work is the trust that is necessary and is established between agents. Nobody wants to accuse a fellow agent, and the security clearances and other mechanisms in place are supposed to screen out untrustworthy types. The field agents, in particular, have been in life-and-death situations together, and supported one another, and thus proven fidelity through deeds to a point where the trust ought not be challenged in mere words. Counterintelligence, which is the business of challenging the bona-fides of both the agents and their sources that they have painstakingly developed, is not likely to be a popular career, nor are its practitioners likely to be popular among the agency branches that they are repeatedly challenging. The cycle is self-reinforcing: unpopular agents get assigned to counterintelligence, counterintelligence agents are unpopular, and therefore that branch of the agency is discredited, and therefore it is an appropriate place to assign those who are perceived as incompetent and unlikeable.

Because counterintelligence at the CIA during this period was powerless and unpopular, the suspicions raised against Ames were never sufficient to lead to a full-fledged investigation, nor were they even shared with the domestic branch of counterintelligence. The agents would protect their own fellows, even one whom they viewed as difficult to get along with and useless in the field. So for ten years, in spite of clear warning signs, Ames' espionage was unchecked. In counterintelligence, Ames had legitimate access to every operation and every agent that the CIA was running in Eastern Europe or the Soviet states. This position enabled him to remove documents easily, in quantities that can best be measured in tens of pounds rather than in terms of individual secret documents. With Ames working in counterintelligence, truly we have an example of the wolf guarding the henhouse. The result was more of a flood than a leak–even the Russians asked him to slow down in 1987, when his handler (half-joking) said, "You know, there's an awful lot of the information that you give us, even though it is very valuable and very interesting, that we simply can't handle."(Betrayal, p. 129) And with Ames in Soviet counterintelligence, there was no immediate other person in a role that would be responsible for finding and stopping him. Even when an investigation was finally begun and had narrowed the search to a few suspects, information about Ames was slow in being collected. For example, an agent named Dan Payne in 1990 did an evaluation of the Ames' finances, and wanted the polygraph test administrators to ask Ames questions regarding the finances. But the Office of Security deemed that information too detailed, and removed all mention of specific dollar amounts from the list of questions for Ames in order to renew his clearance. (see Earley, p.281)

UNDERSTANDING the CONTEXT for COUNTERINTELLIGENCE INVESTIGATIONS

It would be tempting to see this as another example of the good ol' boys' club, similar to stories from various police departments conspiring to hide corruption and incompetence within the ranks. The primary difficulty with this hypothesis is that the history of counterintelligence at

the CIA at most other times during its existence contradicts such a simple explanation. One of the reasons, in fact, why counterintelligence during this time period was so discredited was a backlash against the tremendous power that the counterintelligence branch had wielded for the previous ten years.

The head of the counterintelligence branch from 1954 to 1974 (almost a majority of the agency's existence) was a man named James Jesus Angleton. Angleton is a lesson to be learned about the problems at the opposite extreme of the trust-pendulum from the Ames case. Angleton trusted nobody, and wrecked numerous intelligence operations and the careers of numerous intelligence agents with his paranoia. His dictatorship ended when a new CIA chief, CIA director William Colby[13], eventually forced Angleton into retirement and persuaded Congress to pass the Mole Relief Act in 1979. The Mole Relief Act was designed to provide some measure of compensation for intelligence agents who were never openly accused, but whose careers were permanently sidetracked for one suspicious coincidence or another by the vast power wielded by Angleton. The Act is Congress's affirmation that indeed there is such a thing as excessive paranoia at the CIA, and that excessive paranoia is damaging to the agency and to individuals.

Angleton was in charge of counterintelligence for twenty years. He was prone from the beginning to seeing elaborate conspiracy theories. His paranoia stemmed partly from knowledge of an elaborate KGB operation called "The Trust." At this time, the CIA knew about few operations that the KGB had run, on which to base their expectations regarding their opponent. "The Trust" involved a Russian posing as a dissident, who claimed to have knowledge of and access to a secret rebellion, and he needed Western funding and assistance to build his network. There was no such rebellion, but the KGB used the Western money, weapons, and intelligence information to quell any possibility of one. Angleton developed from this a belief that the Russian intelligence service was monolithic, brilliantly deceptive, and ruthlessly manipulative. His counterpart in the British intelligence community at the beginning was Kim Philby, with

whom he worked very closely, including lunching together almost every day that Philby was in D.C. Philby was a Russian spy, who had been recruited in college and told to enter MI5 or MI6. Both Philby and his handlers were surprised by how far he rose through the ranks before getting discovered. His treachery became known because other members of his spy ring, the so-called "Cambridge Five," were caught, and he fled to Russia rather than risk prosecution. This early experience with espionage seems to have affected Angleton's outlook permanently. He had not suspected Philby, and never again would he make such a mistake. His worst fears were confirmed when a Russian defector (presumed defector–there is still some debate as to whether he genuinely defected or whether he was a "plant") revealed that the CIA had also been penetrated by a mole. The Russian, named Alexander Golitsin, also stated that the KGB would try to destroy the defector's credibility by sending false defectors to share some few tidbits of true information and a large number of falsehoods, in order to keep the CIA distracted and too busy to mole-hunt.

Every possible Russian source thereafter was rejected by Angleton as being a double-agent. On one memorable occasion, a walk-in turned over to the station chief in Russia a series of briefs on Russian assessments of weaknesses of American agents and politicians. The station chief returned the documents to the KGB after Angleton ruled that they were undoubtedly fakes, though Angleton did not see them before making the judgment. The walk-in, we later learned, was discovered and executed. On another occasion, a defector was held in a "safehouse" where the CIA used techniques such as completely isolating him, feeding him only bread and thin soup, and altering his sense of time in an attempt to force the defector to "confess" that he was a double-agent. The cruelty practiced against this Russian defector was one of the stories Ames first recalls when asked why he became disillusioned with the CIA. Remembering the stories about Angleton's molehunt, when Ames became a mole he asked to be known as "Kolokol," (Russian for "bell," a warning) and he always signed documents "K." Ames was Angleton's

nightmare personified. The mole Angleton had looked for so obsessively eventually was created, partly by Angleton's own doing.

Golitsin gave vague clues about the identity of the mole within the CIA as well. He thought the name began with "K"–though whether that was the agent's actual name, or the code-name assigned by the Russians, or perhaps a code-name under which he worked for the Americans, he couldn't guess. He thought the agent was associated with Germany–had been stationed there at some point, or perhaps was originally from there. And he insisted that the agent had "something Slavic in his background." Though in truth, any U.S. intelligence agent at that point in history probably satisfied that criteria, by dint of having worked with the Russians or against the Russians or served time in Eastern Europe or even just speaking Russian, which many CIA agents did at that time. Angleton, working largely alone and later only with the help of an extremely small staff, compiled lists of agents who satisfied one or more of the criteria. The lists ran to several hundred names, a significant portion of an agency that at that time numbered less than 20,000 active field agents. His lists of suspects were never made public, even within the agency. Instead, when the head of any branch considered whom to promote, or whom to move to a new location, or whom to assign a new operation, he always had to clear the choices with Angleton. And Angleton, through innuendo and implicit threats, would ensure that those on the lists could do no harm because they were to be given no meaningful work within the agency. Anybody who opposed Angleton–suggesting, for example, that maybe Golitsin was making this up–was automatically a suspected double-agent, trying to divert the mole-hunt.

The CIA was really a fairly small agency at the time, only 100,000 employees in 1962. It did not take long for Angleton's suspicions to infect the rest of the agency. Employees speculated endlessly about the mole in the agency, but only with the one or two others whom they most trusted. Increasingly, others were looked upon with suspicion. The entire Eastern Europe division was paralyzed. They couldn't trust any new source that might be developed,

and anybody who had ever worked there couldn't be trusted with access to any secret information. No new operations were begun in relation to Eastern Europe during the entire decade from 1963 to 1973. During the height of the Cold War, the most relevant branch of our intelligence agency was effectively out of commission, because of Angleton's paranoia.

Another sign of the paralysis induced by Angleton's radical suspicion can be seen in the output of the counterintelligence office itself. During the period from 1963 to 1973, not even one single espionage case was prosecuted. The list of espionage suspects was extensive, yet of the hundreds of suspects, only in one case was there sufficient evidence to support an administrative inquiry that got the FBI involved. The FBI investigated that individual for eight years, and never was able to produce sufficient evidence to persuade the Justice Department that arrest or prosecution was warranted. The absence of espionage cases during this time period (in contrast to the ten years prior, and particularly in contrast to the period of the 1980s) is so glaringly obvious that the CIA feels it necessary to make a statement regarding it in all of their training materials. Their Security Research Center "Summaries and Sources" manual is used to educate employees of all national-security-related organizations regarding the ways "many of the disasters described herein might have been avoided if concerned co-workers, recognizing danger signs, had been willing to intervene." The third paragraph begins by justifying the label "recent espionage cases:" "The year 1975 marked the end of a ten-year period of quiet in the active prosecution of espionage cases. The government decided to resume an aggressive prosecution of arrested spies in the mid-70s: within ten years, the number of cases brought to court each year had risen to nearly a dozen." (p. ii) That "government decision" represents more probably that the counterintelligence division had finally become functional again after the tenure of Angleton.

The suspicion and lack of trust during Angleton's reign grew, like a Frankenstein monster, out of the control of its creator. Before the end, a new recruit just finished with training, who began working as an errand-runner for Angleton, concluded that the only

possibility remaining was that the mole was Angleton himself, and that Angleton had been running a complex deception designed to deliberately paralyze the CIA and provide the most perfect cover imaginable for his own espionage. "The fellow doth protest too much," so to speak–and that document laying out the case still remains, classified, in the CIA's library. Angleton also of course managed to make a great many enemies during his time as chief of counterintelligence, so that when the new director was appointed his reign was already effectively over. He had "cried wolf" so many times that agents had begun to find ways to circumvent his authority in order to attempt to get things done.

ESPIONAGE RHETORIC AND PARANOIA

Angleton's pattern of reading any and all evidence as proof of espionage is an example of the potential for destruction that is inherent in the paranoid style. The paranoid style has been most often recognized on the level of national politics, following Richard Hofstadter's lead in his 1965 essay "The Paranoid Style in American Politics." The paranoid style results in elaborate conspiracy theories, so that individuals or organizations that are characterized by this style of rhetoric tend to comprehensively frame their perceptions of every event. Hofstadter characterizes the paranoid style as follows:

> "In the paranoid style, as I conceive it, the feeling of persecution is central, and it is indeed systematized in grandiose theories of conspiracy." (p. 4) "It represents an old and recurrent mode of expression in our public life which has frequently been linked with movements of suspicious discontent and whose content remains much the same even when it is adopted by men of distinctly different purposes." (p. 6) "... the central preconception of the paranoid style [is] the existence of a vast, insidious, preternaturally effective international conspiratorial network designed to perpetrate acts of the most fiendish character." (p. 14)

We see evidence of these characteristics in the case of Angleton, and of counterintelligence work more generally. To believe that every single individual who attempts to defect from Russia is in fact a double-agent, sent to distract from a single true defector, is to believe that the Russians had

an almost supernatural mastery of a great many, very complex set of individuals and events. Similarly in more recent times, some of the more complex hypotheses floated by the intelligence community regarding the war in Iraq reflected the same paranoid style. Some intelligence analysts suggested that Saddam Hussein was dead, somebody else had taken control, and was forcing one of the body-doubles to make regular speeches so that the Americans continued attacking until taking out some rival claimant for power. The hypothesis was entirely possible, but it represented so many layers of Machiavellian forethought and control over so many circumstances that only the somewhat paranoid would think of it. And that, of course, is the point of counterintelligence–to think of alternative explanations given an assumption that "all is not what it seems." (The motto of the International Spy Museum)

Hofstadter goes on to note the persuasive power inherent in paranoid reasoning. The paranoid style appeals powerfully because it is both internally consistent and thus seemingly rational, and because conviction shows the believer to be the opposite of naive, which often gets taken for wisdom.

> "Let us now abstract the basic elements in the paranoid style. The central image is that of a vast and sinister conspiracy, a gigantic and yet subtle machinery of influence set in motion to undermine and destroy a way of life." (p. 29) "Decisive events are not taken as part of the stream of history, but as the consequences of someone's will. Very often the enemy is held to possess some especially effective source of power." (p. 32) "One of the impressive things about paranoid literature is precisely the elaborate concern with demonstration it almost invariably shows. The very fantastic character of its conclusions leads to heroic strivings for 'evidence' to prove that the unbelievable is the only thing that can be believed. ... Paranoid literature not only starts from certain moral commitments that can be justified to many non-paranoids but also carefully and all but obsessively accumulates 'evidence'. Paranoid writing begins with defensible judgements. ... The typical procedure is to start with such defensible assumptions and with a careful accumulation of facts, or at least of what appear to be facts, and to marshal these facts toward an overwhelming 'proof' of the particular conspiracy. It is nothing if not coherent–in fact, the paranoid mentality is far more coherent that the real world, since it leaves no room for mistakes, failures, or ambiguities. It is, if not wholly rational, at least intensely rationalistic." (p. 36) "What distinguishes the paranoid style is not, then, the absence of verifiable facts (though it is occasionally true that in his extravagant

> passion for facts the paranoid occasionally manufactures them), but rather the curious leap in imagination that is always made at some critical point in the recital of events. ... What is missing is not veracious information, but sensible judgement." (p. 37)

An organization dedicated to espionage cannot exist without some of the characteristics of the paranoid style. But the difficulty is establishing what should count as "sensible judgement." "Sensible judgement" is clearly a rhetorical matter, and it differs widely across contexts. In the world of counterintelligence, "sensible judgement" is likely to be more paranoid than in the context of civic life generally, where usually the best course for interpersonal interpretation is to assume people mean what they say (again, following Habermas). In other contexts "sensible judgement" might seem paranoid, with the same emphasis on evidence and global explanation and internal consistency, but without the construction of an external enemy. The elaborate, counter-intuitive theories of quantum physics provide an example of seemingly paranoid reasoning that eliminates the threat construction. Just like with any good conspiracy theory, there is a great deal of evidence accumulated to support the hypothesis that hidden forces are at work determining events that we can observe, and that those observable events are not explainable without recourse to these hidden forces, but once the hidden forces are understood then all events can be explained in terms thereof. The hypothesis is all-encompassing. And whether "sensible judgement" can sufficiently differentiate between quantum mechanics and a belief that masterful Russian spies (or today, Islamic terrorists) are manipulating all the events occurring in the U.S. seems like an open question.

On the other hand, it's vital to make the attempt to differentiate between paranoid reasoning and reasonable judgement. The paranoid style can be destructive not just at the level of the organization that is paralyzed (like the CIA under Angleton), but also at the level of civic life. Paranoia can destroy the very possibility of civic (civil) engagement. The paranoid style involves an excess of suspicion, an erosion of trust. The opposite of trust is paranoia. But

without trust individuals and organizations cannot function in an interdependent world. The paranoid style functions to eliminate the potential for compromise or common ground with those who do not share the belief in the conspiracy. Thus use of the paranoid style is antithetical to the functioning of democracy, or of any consensus-based society. The paranoid style, and espionage rhetoric which almost inevitably partakes of the paranoid style, fosters distrust between fellow-citizens and reliance instead on a central authority that has mastered all the levels of secrecy. The central authority cannot be questioned or understood, because the layers of secrets and manipulation necessary for survival shut out all but the inner circles of the elite. Farrell notes the destructive power of the paranoid style in Norms of Rhetorical Culture:

> "The rhetoric of conspiracy and paranoia poses one of the more direct challenges to the integrity of appearances. For in this discourse, what presents itself as public, visible, knowable, and benign is always a lie. For the conspiracy theorist (or in McCarthy's case demagogue), only the hidden is true. And the hidden is always private, invisible, removed from our grasp, and–above all–thoroughly malignant." (Farrell, p. 40)
> "The outcome of a successful conspiracy rhetoric is a kind of counter-deliberative stance... This discourse can never really prove anything, because its ordinary materials are lies. Hence it arouses not faith, but only radical suspicion. It can suggest no provisional judgement or action because the particulars of the world have already been appropriated.... Finally, this discourse must beg, and eventually circumvent, the whole question of virtue.... The question is whether such a rhetoric of 'anti-appearances' can be subjected to the force of prudential reason within the public realm." (Farrell, p. 41)

The question that Farrell ends with is ironic, given the amount of public discourse which addresses conspiracies in cases of espionage. His overall argument is valid, addressing the difficulty of applying standard deliberative norms when the heart of the subject remains secret. In practice, how do individuals make decisions regarding who and what to believe in the context of intelligence work?

BUILDING TRUST in a CONTEXT of PARANOIA

At the level of the organization, the paranoid style is also destructive. An organization

cannot exist if there is not trust between the members of the organization. Trust, in terms of organizations, is actually a rather problematic term. For an exploration of trust and its essential role in organizations, see the edited volume Trust Within and Between Organizations: Conceptual Issues and Empirical Applications by Lane and Bachmann. According to Lane and Bachmann, trust can be established on the basis of shared values[14], on the basis of predictability[15], on the basis of a shared history together in which both predictability and shared values can be developed, or through some combination of these approaches. Given that there will always be uncertainty regarding the behavior of others, and given that cooperative action, any action that requires the involvement of more than one party, requires that one or both parties engage in behaviors that leave them dependent in some sense on the behavior of the other party, trust of some kind is the only viable basis for interaction. The greater the level of interdependence, the greater the need for trust. In a close-knit organization, one where the participants invest extensive commitment, time, and emotional energy, this trust is even more apparent and essential. When matters of life and death are involved (as they often are for intelligence operatives), you have to trust the competence and intentions of every other individual within that organization. The dynamics are easy to see in hospitals for instance, where any outsider can tell at a glance which individuals are used to working as part of the team and which are not. The dynamic is reliable enough that team-building exercises are deliberately chosen which will potentially imperil the lives of the individuals, as when the new management-trainee-teams go cliff-climbing together. Without trust, an organization cannot function, and without being able to function the organization's reason for existence ceases, and it will come to a rapid end.

Trust is the single most critical issue for the functioning of an intelligence agency. Who can be trusted? Who cannot be trusted? In the world of espionage, you have to assume that deceptions abound at every level. The "enemy" has counter-intelligence forces at work always,

or at least that must be the operating assumption. But as the Angleton case suggests, paranoia of this sort can be destructive. If you cannot trust your teammates within an organization, then that organization cannot function. If you are suspicious of every individual you work with or meet, then you're not a useful intelligence agent, because you can't afford to take risks given the high degree of interdependence and uncertainty.

Functionally, intelligence agencies rely on numerous rituals to safeguard their membership, and these safeguards enable the level of trust that is necessary for agents to trust one another, oftentimes even entrusting them with their lives. Sometimes the entrusting of lives is literal, sometimes it is a metaphor for employment, and sometimes rhetorically it's a part of the selling of the importance of intelligence work, for here is where it is not just individual lives being entrusted but the lives of "all Americans." Trice and Beyer (1984) argued that all organizations make use of rituals, and that the most common types of organizational rituals tend to fall into five categories. A ritual is defined as a set of symbolic (hence communicative) practices designed to simultaneously both create and mark a change in a social reality. The five most common types of rituals are integration, degradation, enhancement, renewal, and leavetaking. Here we have an example of an integration ritual. The rituals of the CIA create a social reality that includes an insider/outsider dichotomy and an internal community that has been made into one that is safe and secret and therefore trustworthy.

Trust through Code Systems

One such safeguarding ritual is the use of codes. Codes are important for protection from the prying eyes of outsiders, but they're also vital to identify legitimate insiders to one another. Spy codes are one of the characteristics most closely identified with the intelligence community, and public fascination with the cryptographic practices of the community is one of the constant characteristics across all discourses related to the genre.[16] Using codes is not a ritual that is unique to intelligence communities, of course. Codes are a constant whenever there is a group of

insiders that must be able to recognize or share meanings with each other while excluding outsiders. Persecuted minorities develop code systems, for example[17], but on a smaller scale the development of codes as rituals can be seen even in couples or groups of friends.

Trust through Mutual Understanding Based on Shared Backgrounds

The use of codes is one form of safeguarding ritual, but there are others such as the practice of drawing agents from a uniform background. Having shared backgrounds reduces their uncertainty about one another, and thus enables trust to be more rapidly developed. The traditional difference in personnel backgrounds between the CIA was one source of the tension and lack of cooperation between the agencies. The CIA was historically was primarily military personnel, who rose through promotion during combat, and the State Department was historically primarily Ivy-League educated, with all of the characteristics that accompanied that class. The history of the CIA shows progression closer into alignment with the State Department and more clearly differentiated against the FBI over the course of its fifty-year existence to date. The history of the CIA does not show much increase in diversity in its membership until very recent years (essentially, post 9-11). The problems with establishing trust by relying on shared backgrounds has become painfully obvious. The organization lacks the variety of resources to adapt to operating in new contexts, or to change practices that have become dysfunctional.

Trust through Heightening Insider/Outsider Differentiation

A third safeguard, the most highly visible of them, is the use of security-clearance procedures such as the conduct of a "background check." Security-clearance background checks are a ritual meant to reassure the public and the individuals employed. A typical background check takes anywhere from three to six months, and in terms of manpower costs approximately $60,000. The check involves a series of interviews asking the candidate questions about political views, drug use, group affiliations, and personal lifestyle, including delving into the individual's sex life. Historically, homosexuality was often viewed as a sign of future betrayal, but other

sexual deviations that might enable a blackmail strategy to succeed were also being screened for. The check also involves an investigation of the individual's entire financial history. The third strategy in the background investigation involves interviewing individuals who might have been in a position to know something of the candidate's finances, personal lifestyle, drug use, political views, and group affiliations. Landlords, employers, family members, former roommates, former romantic partners, all get located and queried as part of a background check towards gaining security clearance.

We will never be able to estimate the effectiveness of the background check. We cannot even estimate the rate of false-positives (i.e., those given clearances who should not have been given clearances) with any reliability, because any guesses would be based on assuming that we catch every (or almost every) instance of betrayal, and surely to believe that is a sign of the hubris that leads to tragedy. And the rate of false-negatives (i.e., those denied clearances who would not have been guilty of betraying that trust) is probably quite high, and of course unknowable, being counter-factual. Many of the scholars who have studied security clearances and issues of betrayal note that this is entirely the wrong way to think about espionage anyway. The theoretical model that puts security clearances in place assumes that "tendency towards espionage" is a personal characteristic, a fairly stable trait that can be possibly detected if it is present. It makes as much sense to assume that espionage is largely a product of the environment. Environmental characteristics such as ease of access, low estimated probability of getting caught or punished, high rewards for betrayal (though the rewards might not be monetary or other easily-recognized forms), available and readily apparent opportunities for transport, and other factors in a specific situation might increase the probability of espionage. The weakness of explanations based on environmental factors necessitates some role of individual personality. In any single group that shares basically the same environment at work, some individuals might be

guilty of espionage while others will not. Even if we do accept that tendency towards espionage depends at least to some extent on individual personality characteristics, those characteristics might change over time. Assuming that the personality characteristics which increase tendency towards espionage are stable over time is a necessary assumption to support the background-check model, because otherwise there is no theoretical explanation to support belief that prior history would provide indication of future espionage. We see in practice however that people change, and in fact many aspects of personality change dramatically over the course of a person's life and across situations. Why should we not assume that inclination towards espionage might not also change?

The intelligence establishment is long and well acquainted with these arguments. Why, then, do agencies continue to invest the kinds of money and time necessary for background checks? Why do they continue to tolerate the many false-negatives that deny potentially valuable employees to the agencies that might need them, and deny individuals an opportunity for a job they perhaps really wanted? Part of the answer may be that the background checks serve as a necessary ritual, a fragile bridge across which trust can begin to be established.

In fact, security clearances serve as a necessary and essential ritual for intelligence work in two ways: security clearances provide a sense of reassurance, a reason to trust the new employee for both the current employees and for the government and tax-paying public. They also serve as a ritual to heighten individual commitment to the group. It is well known that the more difficult a group is to join, the more any individual who joins will feel commitment to the group. This well-known phenomenon accounts for the widespread practice of "hazing" new fraternity members, and for why exclusive groups or groups that have a high membership fee often experience greater member commitment. The security clearance and background check serve as an obstacle, demanding a price from not only the employee but also imposing a price on their family and friends. The donation of the time spent being interviewed also guarantees that

those close to the individual will also be aware of the seriousness of his/her new responsibilities. We reduce the likelihood of espionage by turning those closest to the employee into watchdogs, who themselves committed time and effort to winning him/her the security clearance. One of the striking characteristics of espionage investigations is how effective this process of creating watchdogs is. Out of 105 espionage cases, seventeen have been discovered only because a close friend or family member alerted an investigating agency that their loved one had turned traitor. The individual seeking employment is also put through a ritual that is handled with great seriousness, putting him/her on notice that the new responsibilities ought to be taken very seriously indeed, that National Security is on the line.

There are thirteen criteria involved in a background check. The criteria have been standardized across all federal agencies that involve security clearances, and codified into a reference manual. Much like any other field of law, the regulations that determine whether or not a security clearance will be issued are clarified through the accumulation of previous cases. The similarity between background check procedures and legal procedures is not coincidental, because the denial of a clearance is denial of employment, and therefore potentially subject to litigation. Such legal cases are seldom prosecuted, and even more rarely won. Stated in their strongest form, the thirteen criteria are nearly impossible for an individual to meet. Few people will actually meet all thirteen qualifications perfectly, and certainly there are not enough individuals who would meet all the criteria perfectly to be able to fill the employment needs for all positions that entail a security clearance. This is particularly true today, given the tremendous volume of classified material dealt with and produced each year. [Include some stats ??? here about said volume, and number of individuals with clearances] To address the need for some flexibility in the background check criteria, ameliorating factors have been introduced. Security clearances are handled by the Defense Security Service. The list of criteria, along with mitigating factors and a list of automatically disqualifying conditions, is made available in a

form called the "Adjudicative Desk Reference" or ADR. The manual describes all thirteen criteria in terms that are sufficiently broad and ambiguous that a legal proceeding arguing that clearance was wrongfully denied is unwinnable. Each criterion has an initial phrase labeling the criteria for shorthand reference. This phrase functions in much the same way that we refer to specific constitutional amendments in shorthand form rather than by number: the "due process" clause, the "cruel and unusual punishment" clause, for example. Therefore in the list I provide here, those same labels are used, even though they lack parallelism and do not specify in short form exactly how they relate to national security. The mitigating conditions are also defined broadly, leaving the specific personnel in charge of hiring with wide discretion. The thirteen criteria are as follows:

1. Allegiance to the United States. This criterion functions in both a positive and a negative form, in that the applicant must show behaviors which indicate allegiance (willingness to recite the Pledge of Allegiance, for example) and not show any behaviors that would show lack of allegiance. Historically, there have been tensions over whether criticizing the federal government shows lack of allegiance, as when an individual participates in peace protests. The negative form of this criterion has been by far the most problematic of any criteria. The official ADR actually has a nice reminder about freedom of speech, including references to court decisions deciding the limits of sedition, in an attempt to resolve some of these ambiguities.

2. Foreign Influence. This criterion functions negatively, meaning that the individual must not show any signs of potential to be influenced. This includes any friends, family, or business interests in any foreign country, whether or not they are allies of the U.S.

3. Foreign Preference. This criterion is closely related to Foreign Influence, but extends the requirement. Not only can the individual not be vulnerable to foreign pressures because of direct personal involvements, they must not be vulnerable based on liking. This forbids behaviors such as any statements or activities that indicate a positive attitude toward any foreign

government or people, whether or not they are allies.

4. Sexual Behaviors. Almost any non-mainstream activities can be disqualifying. The ADR focuses discussion most extensively on homosexuality, promiscuity, swinging, exhibitionism, and extramarital affairs. The concern over non-mainstream behaviors is partly due to fear of blackmail, partly due to fear that if a foreign intelligence service learns of any sexual deviance they will use the knowledge to seduce or offer sexual rewards in return for information, and partly due to historical misperceptions. Homosexuality was at one time considered a mental disorder and was believed to be linked to treachery, and high-profile cases such as Guy Burgess and Don Maclean (two of the Cambridge Five) reinforced negative stereotypes. The current version of the ADR goes to great lengths to refute such misconceptions, but continues to consider this a potentially disqualifying factor based on the first two fears.

5. Personal Conduct. This is one of the most vague criteria, which generally functions negatively. The conduct referred to includes behaviors such as dishonesty, irresponsibility, failure to follow rules, or poor personal judgement of any sort.

6. Financial Considerations. This criterion can be disqualifying on the basis of either too much debt, or too much income from unexplained sources.

7. Alcohol Abuse. Historically, the CIA and the FBI have both been considered hard-drinking cultures, and so the distinction between what is considered use and abuse varies widely. Officially, any evidence of any intoxication problems is disqualifying unless treatment was sought and successful, because of the strikingly high correlations between spying and alcohol and the high availability of alcohol in the field agent's lifestyle. Attending official ambassadorial functions and recruiting agents there demands an ability to drink without losing good judgment.

8. Drug Use/Abuse. Any evidence of using an illegal drug can be considered disqualifying, but in practice certain drugs are more the subject of concern than others. The

ADR particularly focuses on cocaine, heroin, or any hallucinogen as reasons for concern. Cocaine and heroin are problematic because of their addictiveness, and hallucinogens are problematic because the essence of intelligence work is observation, which cannot be trusted if the agent's perceptions are effected by drugs.

9. Mental, Emotional, or Personality Disorders. Any signs of a disorder of any kind can be considered disqualifying, whether or not the individual has been officially diagnosed. Mitigating circumstances include the question of whether the disorder is treatable through medication, or a professional declares the individual "cured." The ADR particularly focuses on disorders that might be the subject of blackmail because they are socially frowned upon, and those that might render an individual vulnerable to manipulation.

10. Criminal Conduct. This criterion functions negatively, in that any felony and almost any misdemeanor can be considered disqualifying. The reasoning is based upon concern not with the crime itself, but with the crime as an indication of lack of respect for authority. This is a particularly interesting criterion for the FBI, whose charge historically has been fighting crime domestically. The ADR focuses particularly on crimes which show lack of control such as assault, and on misdemeanors regarding firearms.

11. Security Violations. This criterion includes not only information security, but also personal security risks or endangering the security of others. Behaviors such as propping open a fire-escape door or disabling smoke-alarms in one's apartment would be considered concerns, though not necessarily disqualifying.

12. Outside Activities. This is a negative criterion, in that any outside employment, membership in certain volunteer organizations, or hobbies that might "influence judgment" are considered potentially disqualifying. The reasoning is based on a fear that any activity to which an individual commits significant time might have a higher priority than national security considerations, and the ADR specifies that this is of particular concern if those outside activities

might be infiltrated by foreign agents.

13. Information Technology Misuse. This is the most recent of the criteria, and broadly defined. "Misuse" can include allowing another person to access your account, using a work-related account for non-work-related purposes, excessive time spent online, "flaming" another on e-mail or on a discussion group, or visiting websites of questionable legality or propriety. This criterion has been particularly emphasized in light of the increasing role of information technology in espionage cases.

Clearly, the thirteen official criteria for a security clearance have not been able to prevent espionage in the past, and one could argue that a clever and prepared spy would be able to satisfy the criteria more effectively than a loyal but average American citizen. The list is by no means foolproof. Yet it is a ritual to enable trust within the community and for outsiders. But trust is also a form of voluntary blindness, a decision to read ambiguous signs in the way most favorable to the individual sender. And a strong bond of trust between individuals in an intelligence agency can provide the very environmental characteristics that are most likely to lead to situations of espionage. Consider, for example, the case of Aldrich Ames.

EVIDENCE AND EXPLANATION in the Ames Investigation

Ames could easily have been caught when he first began selling secrets to the Russians. The first secret he sold is still a contested issue, in that Ames tells a different story than his Russian handlers tell. It is agreed that the first secrets, for which he was paid $50,000, were the names of three intelligence agents. Ames claims that they were the names of three double-agents; that is, agents working for the KGB, pretending to sell secrets to the CIA in order to spread disinformation and learn more about how the CIA operated. Only a month later, he sold all at once the name of every U.S. agent operating in Russia. His motivation is not entirely clear. His own explanation, given in CNN interviews and interviews with his biographer, is that he

was worried because a mole working for the CIA in the KGB might have found out about him, and betrayed him. The Russians silenced every single agent ("human asset," in intelligence lingo) that was on Ames' list. Most of them were executed, though in one way or another a few were able to escape. For example, the most famous of the agents was Oleg Gordievsky, who was actually working for MI-6, and whom the British rescued from the center of Moscow despite the surveillance kept on Gordievsky. The rescue, pulled off in 1984, was the very epitome of the daring James-Bond-style British intelligence agency at its best. A few of the agents Ames betrayed were questioned and imprisoned by the KGB but later released, when Yeltsin came to power and proclaimed a general amnesty. All of the Russians whom Ames named were never again able to contact the CIA, and so our entire network of sources inside the Soviet Union was essentially lost all at once. Of those agents whom we know did not survive, rumors abound regarding the method of execution for some of the agents betrayed. Later defectors have suggested that at least one was executed by being lowered slowly into a furnace with a class of new KGB agents watching. KGB records do not support this rumor, and General Solomatin, a more recent defector and former head of the KGB, insists that the Russians always used bullets for executions.

The fact that so many agents were rendered inoperative all at once was too striking to be purely coincidental, and a massive investigation was begun almost immediately[18]. But the investigation was slowed by numerous alternative hypotheses and numerous intervening events.

Explanations Flawed Due to Delimiting the Data Too Broadly

The investigation was sidetracked first by the evidence that was recovered from the last drop of the first spy killed (Sergey Ogorodnik). He had photographs, using a miniature camera given to him by the CIA for this purpose, of documents purporting to represent a conversation between out-going Secretary of State Henry Kissinger and his Russian counterpart, in which Kissinger instructed the Russians how to manipulate the next round of missile talks (leading to

the Salt II treaty) to their advantage. Were the documents fake? Or was Kissinger committing treason in his resentment at losing his position?

The investigations were unable to resolve questions as to the authenticity of the documents, and conveniently the relevant strip of film and all related documents eventually disappeared. Ames later went searching for it, once he had access as part of his counterintelligence work. The investigation returned to the central question of "why did we lose so many Russian agents all at once?" Espionage clearly had to be one possibility that needed to be considered, but an alternative explanation was the preferred hypothesis: the Russians perhaps had developed a new technology that enabled them to eavesdrop on all electronic communications in and out of CIA headquarters.

Explanations Based on the Mysteries of Technology

There were many good reasons to assume that eavesdropping was possible. For one thing, the CIA had for years been eavesdropping electronically on KGB headquarters, because during the construction the CIA had bribed an electronics technician to place a "tap" on the phone wires. This was one of the secret operations that Ames sold information regarding. For another thing, a Soviet claiming to have been friends with one of the agents executed offered to sell us information as to how the agent had been discovered, and had said that the electronics were the source. So this was a logical hypothesis, one that could be tested. The head of the Soviet division arranged for messages about a "new KGB recruit" to be sent back and forth. The KGB agent named was never questioned. This test didn't completely falsify the theory of electronics being the source of the leak, but now human intelligence also clearly had to play a role as well.

Another hypothesis is that there was a combination of some espionage, perhaps low-level, along with mistakes in using tradecraft made either by the CIA or by the Russian sources themselves. Tradecraft refers to the collection of procedures, equipment, and symbolic actions

that are unique to a particular intelligence agency. If we accept a broad definition of technology, which includes specialized procedures, then again this hypothesis amounts to an explanation appealing to flawed use of technology. This hypothesis was supported in part by the inclusion of all cases of losing Russian assets, even some that happened significantly earlier, such as TOPHAT and FEDORA, cases which we believed we knew had been revealed by our own side.

As rhetorical scholars, it is worth pausing for a moment in considering this hypothesis to analyze critically its persuasive effect. Bear in mind that the CIA investigation proceeds by means of written documentation, and all communication suggesting hypotheses to be investigated will follow the norms of writing. This first hypothesis was investigated initially, presumably because it was viewed as the most probable at that time. Why was it viewed as the most probable? In part because in writing the hypothesis, persuasive effects that were not necessarily intentional were impacting the readers. The practice of writing the code-names of agents, meetings sites, and operations in all capital letters is standard within both the CIA and the FBI. I don't know where or why the practice first developed, but not only are agent codenames capitalized, all operations are named and the names are written in all capitals, as are specific documents or procedures. The capitalization has the effect of drawing attention to agents' code-names every time they are mentioned in a document. Agents are almost never referred to by their true names, even in cases where those are known. Code names are used even after a Soviet source has publicly defected and his name has been published in newspapers. Notice that the effect this has is to highlight the elision. The capitalization has the effect of emphasizing the adherence to secrecy. A document which uses one or more code-names asks each reader to participate in its secrecy by filling in the missing information if they can. Those who can, are continually reminded that they are part of an elite, a secret group with knowledge not shared by others. Those who cannot fill in the missing information are reminded that they are not "in the know," that there are secrets in the inner sanctum that vouchsafe credibility to the

secret-keepers. The constant reminder functions a bit like the secret handshakes developed by fraternities, or the secret symbol-systems that led to such suspicion regarding the Free Masons.

Explanations Based on Blaming the Victim

The director's special investigator, John Stein, studied each case, and in all of the early cases it was distinctly possible that mistakes had been made. In one case, it was known that the agent had stopped and had a drink or two before going to the dead-drop site. In another case, it was known that the CIA handler might have been able to be traced through a technology that the Russians called "spy-dust:" a chemical that was invisible without special glasses, but which allowed them to trace where the Americans went and who they interacted with. The fact that potential mistakes could retrospectively be noted in almost every case is probably not surprising: after all, human nature is such that a constant guard against errors of every kind will in all probability fail in the long run.

A Russian defector named Vitaly Yurchenko also provided a new hypothesis. Edward Lee Howard, a CIA employee who worked for a very brief time during 1983 in Moscow, had been fired for having falsified information on his background security check. In his resentment, Howard had sold everything he knew to the KGB. Howard was placed under surveillance, but before he was arrested he made a daring escape in which, as his wife drove them both home after dinner, he rolled out of the passenger door while going around a corner. His wife immediately slid a life-size dummy into place as he did so, so that the CIA agents trailing them would still see the silhouette of two individuals in the car. Howard escaped to Russia, and so the CIA was never able to question him and learn exactly what information he had gained access to, and what he had sold. In fact, it is likely that several of the agents whose names Ames sold, had also been betrayed by Howard, who had been trained to pass messages from and to them.

Yurchenko himself was perhaps something of a red herring. After a few months living in a safe house and being debriefed by the CIA, in the person of Ames himself, Yurchenko re-

defected with much publicity. He claimed the CIA had drugged and kidnaped him, and he went home to Russia without being penalized in any way. Was Yurchenko in fact a double-agent, meant to distract the CIA and mollify them that the only mole had already been dealt with? The debate is difficult to resolve, since any answer the KGB provides must be suspect. They could lie if they say that he was a double-agent in order to claim credit rather than have one more Russian defector. Or they could lie if they say that he was not a double-agent, in order to preserve his cover and perpetuate the disinformation he gave the CIA. Or they could be telling the truth either way. Yurchenko himself could probably not resolve the debate, but regardless he has steadfastly refused to speak to Westerners since his return home.

Explanations Based on the Insider/Outsider Dichotomy

A third hypothesis explaining the loss of the Russian assets attracted much public attention, and diverted the investigation away from Ames. One of the Marine sergeants, Marine Sargent Craig Lonetree, responsible for guarding the U.S. embassy in Moscow admitted to having sold stolen secret documents, specifically the fire-escape plan for the embassy. The Naval Investigative Service took the unprecedented measure of recalling every Marine on duty during that time, and during a sixteen-hour interrogation session, extorted a confession from one of them that KGB agents had been admitted into the building. If KGB agents had access to the building, it was possible that any secret mentioned in any document could have been stolen. But the Marine later recanted his confession, claiming that he had been coerced into confessing, and NIS eventually dropped all charges, unable to find any other evidence that KGB agents had gained access.

In addition to the difficulty of figuring out why so many agents had been silenced, the CIA had hurdles to overcome in determining whether or which agents were in fact executed or imprisoned. The KGB was unusually secretive about the arrests made on the basis of Ames' information. Rather than publicly declaring that a traitor had been caught and punished (the

usual practice, which served as a deterrent and stoked the paranoia that provided the agency generous funding), the agents who were betrayed by Ames were kept imprisoned for a year or more before being executed, and when possible the executions were kept secret, though it is harder to keep an execution secret than an imprisonment of a man who is expected to be serving secretly in another country.

Obstacles Precluding Explanation due to Pressures from External Priorities

The CIA mole-hunt met another obstacle as well, in the form of the Iran-Contra hearings that began in 1986. The hearings demanded much of the attention of the top administrators in the agency. Thus the mole-hunt became a priority only for those at the lower levels, particularly a tenacious agent named Sandy Grimes, who was herself in charge of handling two recently recruited Soviet agents, and the librarian, Jean Vertefeuile.

As the Congressional hearings later pointed out, we have here a problem in which the mole should have been discovered much earlier, but all the evidence was read to support alternate hypotheses. We have here the opposite of the problems that occurred in the Lee case: For Lee, incomplete evidence led to a leap with the assumption of espionage. For Ames, incomplete evidence led to a leap assuming there must have been an alternate explanation. Why the difference? Various factors contributed to the difference. Ames was a group member, and nobody wanted to assume his untrustworthiness. China was a threat that was politically viewed as increasing, while Russia was a threat that was even then on the decline. Additionally, with the separation of responsibility into separate agencies, Trulock and his group stood to benefit from finding a spy, while the CIA as all one agency stood to be discredited if they found a successful spy. Of course, in the event they stood to be discredited much more severely for NOT finding the spy in their midst. Indeed, the CIA came under very heavy criticism when the Ames case finally came to light.

LESSONS LEARNED

Congressional hearings into the Ames case focused on a variety of interrelated questions: how was Ames able to do so much damage, and the related question of why was the agency so slow to find Ames? What damage did Ames do? And as a related question, what was the value of the information that Ames gave away? Their conclusions were for the most part sharply critical of the CIA. The hearings were led by Sen. DeConcini, but the criticism of the CIA was led by Sen. Patrick Moynihan, who had been arguing against the excessive secrecy of the agency since 1987, in the wake of the Iran-Contra hearings. Moynihan had been battling against the CIA on the basis of excessive secrecy, which he believed was hurting the government's ability to control the CIA and even conduct foreign policy. Moynihan had a long list of examples to support his accusations about excessive secrecy, having served on the Senate Oversight Committee for eight years, and in that position having access to any materials desired. Moynihan was fighting a two-front war: he battled the excessive secrecy of the CIA, but was simultaneously arguing against critics of the CIA who viewed it as dangerous. His conclusions, published publicly in 1997, were that CIA secrecy was banal and largely ritualized, and that the danger was not posed by the magnitude of the secrets themselves but by the posturing and suspicion invoked by secrecy. The Congressional committee after Ames did not come to the same conclusion as Moynihan. The Congressional committee's conclusions were that the CIA was not sufficiently careful regarding who had access to what information. In effect, the problem was not enough secrecy rather than too much. A new classification scheme, "Special Compartmentalized Information," was introduced to provide a level even above that of "Top Secret." Special compartmentalized information could not be shared even with others who had similar security clearances. In other words, no communication regarding this class of information could be allowed with anybody, sometimes not even with supervisors, sometimes not even with others on the team. This enabled truly crucial secrets, like lists of the names of agents operating in Russia, to be protected even against those within the organization. Other

levels of classification also had tighter security measures imposed, in an attempt to prevent the kind of problem that Ames represented.

At the same time, greater communication regarding personnel matters were declared necessary, a result directly contrasting the lesson learned from the Angleton experience. After Angleton, the CIA was left with a recognition that casual sharing of suspicions regarding named individuals was needlessly damaging to agency morale and to individuals and their ability to function productively for the agency. The Ames case taught the need to make sure that criticisms made by one individual of another needed to have some way of being recorded and shared. The lessons are opposite: both more sharing and less sharing of information were required. The paradox bedevils not only intelligence agencies but other organizations as well. The paradox haunts all who handle secret information: in order to protect it, it must reach fewer people, but in order for the information to be worth having it must reach people who have other related bits of information and are in a position to make decisions based on the information. The Ames case highlights the need to protect information. We have to be more and less vigilant at the same time, sharing both more and less information. Today with the war on terror we realize ironically both a greater need for the sharing of information among decision-makers at all levels, at the same time that the government is declaring ever more information secret.

In light of this paradox, consider more recent events. The Congressional hearings after 9-11 were investigating, among issues like airport security and flight schools, what went wrong in the intelligence community. How did we fail to have any intelligence regarding this highly orchestrated attack? The general conclusion was that the various intelligence agencies failed to exchange sufficient information, so that clues which the FBI had and clues which the INS had and clues which the CIA had were never put together. In retrospect, we can see how the clues could have led us to forewarning and perhaps, maybe, even a chance to thwart the attack. But at the time nobody could see the big picture because of insufficient communication.

As one journalist wrote in an article titled "What We Have Here is a Failure to Communicate," "The war on terrorism will be won or lost in the nation's intelligence and counterterrorism agencies." (Josh Micah Marshall, in Blueprint, the newsletter for New Democrats Online) The president's various anti-terrorism measures recognized the need for greater coordination and information-sharing among the intelligence agencies, and attempted to encourage it by removing legal obstacles. For example, previously grand jury testimony collected by law enforcement agencies could not be shared (grand juries, after all, are closed and secret procedures, unlike regular trials). The decision to make such information sharing legal however does not address the structural tensions existing between the FBI and the CIA, and the interagency competition means that even when legal, in practice information is not likely to get shared.

There are numerous reasons for the disinclination to share information. One is technical difficulty doing so. The FBI computer system is decades behind the times. The lack of up-to-date information technology has impacted other espionage cases as well. For example, Hanssen was easily able to hack the system and retrieve any information from it that he desired. The FBI has since then increased computer security, without updating its systems, with the result that the databases they have are now fragmented and incompatible, with firewalls (computer jargon for the software that limits contact outside of the system) preventing coordination of information even inside of the FBI, let alone with other intelligence agencies.

The technological constraints on information sharing are only a small part of the reason, though more easily pointed to than most, why information is not shared between agencies. Lack of trust, given that each organization has its own history of traitors and spies within its ranks, also decreases information-sharing. These are some of the environmental characteristics that tend to increase incidents of espionage. Bureaucracy tends to de-individualize the employees working for any large organization, which makes treachery easier and trust more difficult, a

tendency noted by Weber but implicit even in earlier work by Taylor. But the overriding difficulty in increasing information-sharing between our intelligence organizations consists of the bureaucratic tendency towards secrecy first described by Max Weber. Weber noted that bureaucracies act in order to protect themselves and in order to increase their scope of power and their size. To protect themselves, damaging information is kept secret ("bad news never travels up"), and in intelligence organizations, where secrecy is a virtue, very soon all information is kept secret. The intelligence organizations can't stop enculturating members to see secrecy as a goal in and of itself, for that would presumably increase the probability of agents taking declassification decisions into their own hands. We saw earlier in this chapter that Ames' disgust with the secrecy and its disconnect with policy was one factor influencing his decision to sell secrets. The danger of this perception that secrecy has become a goal in and of itself is that it will lead to a reaction in the opposite direction. The danger of a counter-reaction is not merely hypothetical. In a case like that of Jonathon Pollard, we see individuals making declassification decisions because they see it as increasing national security to end secrecy on a given topic or with another individual/organization/country. The decision gets made against a background in which the valuing of secrecy for the sake of secrecy, and a fear that this is no longer rationally supporting national security. The case of Pollard is an interesting contrast to the Ames case for three reasons. One reason is that, while both are motivated by a disgust with secrecy, the results were vastly different. Another reason is that the public reaction was for the most part diametrically opposite, in that Ames becomes the exemplar of an evil and damaging spy, while Pollard becomes an example of intelligent independent initiative, and clearly highlights questions regarding whether all espionage is treason. The third reason for considering the Pollard case here is that, just as with the Lee case, race becomes a crucial issue for understanding motivation. Pollard and Ames become opposites in the sense that one is an example of ideological motivation while the other is an example of monetary motivation, and the result

contributes to why they are evaluated so differently publicly.

The Problem with Lessons Learned: a Counter-Example for the Ames case in which we visit the openness vs. secrecy question again

Pollard was an intelligence analyst who specialized in Mideast affairs, particularly the tensions between Israel and its neighbors. Israel is and was a strong ally of the U.S., and so Pollard was troubled by the amount of information we collected regarding the region but did not share with Israel. Pollard was, in addition, a Jewish American, which heightened his discomfort with the secrecy between the two nations. So he gave two documents to a friend of his who was serving in the Israeli air force. This is a classic example of espionage for the sake of ideology as it gets practiced in the United States, in contrast to the numerous cases we have of Soviet intelligence agents who made the decision to sell information for ideological purposes but also usually accepted cash in return. Pollard was interested in increasing American security by increasing the strength of its allies and their ties to us, and so applying the label of "treachery" in this particular case of espionage is problematic. The reaction to this case of espionage is unusual. In the mainstream media, the specific harm of the espionage (i.e., who was the recipient of the secrets) was emphasized less than the danger of a spy who was from a non-mainstream background and sold classified information based on his allegiance to others of his race. In the cases of media with large Jewish audiences, though, the espionage produced more criticism of the secrecy practices of the CIA than criticism of Pollard. Just as in the case of Daniel Ellsberg of the Pentagon Papers fame who share secrets with the American public, Pollard was viewed as a hero of "the people" by exposing secrets that the government should not have been attempting to hide. Pollard was able to and willing to engage in espionage because the increase in secrecy in the CIA bureaucracy meant that all the information handled by analysts is classified and the growth of complexity in the Middle East meant that analysts need ever-greater amounts of information in order to be useful for guiding foreign policy.

Why is it problematic that Pollard chose to share information with Israel, one of the strongest U.S. allies and a pivotal nation in an unstable region? Because the CIA uses the information to purchase influence and to purchase other information. Information functions as a market commodity rather than a revealing of internal states or a sharing of meaning towards community building, two other theoretical ways of understanding communication. In fact, the specific information in question, about the purchase of Russian fighter planes, would have probably gotten into Israeli hands eventually without Pollard's intervention. The information would have been held until it could be exchanged for information deemed valuable to the U.S. or for favors like extradition of an Israeli citizen wanted in connection with a crime in America. Pollard's espionage reduces the value of the CIA's product on the information market. The dynamic of value decreasing as availability increases means that the CIA has a vested interested in keeping secrets, for by restricting the supply of information the perceived value of their information increases. The dynamic can be explained by the basic economic principle emphasized by Adam Smith. A clearer understanding of the implementation of the information market could be gained by comparing it to Pierre Bourdieu's notion of cultural capital. Cultural capital, like information used as a commodity, must be created, and is sustained by the operations of power and dominance. The CIA is powerful because they have access to secret information, and the FBI has similar power, whose uses were explored more explicitly under Hoover's guidance. Both agencies keep information secret in order to gain power, in a self-perpetuating cycle.

The intelligence community is left with quite a challenge. There is something of a paradox here: in order to maintain secrecy the agencies must limit distribution of information, but just like in science, information is less usable if it isn't distributed. Lack of distribution is problematic also because it leads to lack of inter-agency cooperation. But to fix the communication problems imperils the secrecy and increases the likelihood of leaks. So what

should be done?

PREVENTING ESPIONAGE

Without attempting to set policy, there are still some perspectives available from a communication perspective that suggest strategies for mitigating the tensions of the paradox. The paradox faced by intelligence agencies is the same fundamental tension between silence and communication, between dialectic and rhetoric, that in other forums have been addressed extensively. What follows here represents some reflections drawing on communication theory applied to the Ames case and espionage more generally.

Strategies Relying on Symbolic Intervention

Textbooks in communication sometimes teach a theory called "Expectancy Violation Theory." One of the aspects of this theory concerns territoriality, both primary and secondary territoriality. Primary territory refers to spaces which we regard as exclusively our own, such as "my car," "my house," even when technically the bank still owns those items. In regard to primary territory, we will behave defensively if violations of that territory occur. The defensive behaviors might be as simple as nonverbals saying "you're not welcome," or verbal behaviors such as questioning the reason for the violation. But the defensive reactions might escalate if the violating behaviors are continued or increased. Secondary territoriality refers to a sense of ownership regarding spaces or objects that we routinely use, even if we are not exclusive users. We can demonstrate that material artifacts become secondary territory and are also defended if an unexpected violation occurs. The secretary becomes wrathful if the stapler is gone from her desk without explanation, even though it is company property and the employee using it is engaged in company business. The seat I use every time class meets in the seminar room becomes "mine," and if somebody else sits there I will likely comment, and expect to be given a reason as to why the violation occurs.

An individual's work environment consists of secondary territory, and in some cases

might come to be regarded as primary territory. This is true even though employees if asked will acknowledge that the company is the legal owner. In many organizational cultures the territoriality is so pervasive that the computer and automobile become "perks," a fringe benefit that is as much part of the compensation package as health insurance and a paycheck. An employee does not need to be on the job for long before beginning to associate objects as territory, either their own territory or the territory of others. An individual will be more likely to regard objects within their work environment as primary territory if they have exclusive use, and particularly if they have had some responsibility for the process of the object's coming into use– selecting which one to purchase, or in some cases producing the object himself. This is likely to be particularly true for "intellectual property" which the employee created himself.

It's also worth noting that the territory of others is marked and respected as another individual's territory. Employees much more quickly come to see objects as the territory of another individual than as the territory of an impersonal, faceless entity such as "the company" or "the government." The secretary's wrath is more likely to be accepted as legitimate than the impersonal prosecution that the company, through it's lawyers, might engage in protecting "their" office supplies.

Looking ahead to the Wen Ho Lee case, for example, he argued he backed up the codes because they were "his" codes, and he felt both responsible for them (even the sections which he had not created) and privileged to do with them as he saw fit. His explanation in "My Country Versus Me" would fit this notion of territoriality neatly.

An employee of the CIA cannot be expected to behave any differently. A long-term employee will probably inevitably come to regard the files that s/he put together, and is officially responsible for, and uses primarily or exclusively, as his or her secondary territory, or even primary territory. The office supplies, the computer in his/her office, become primary territory, and as such any violations will be met with sanctions. Inquiring too closely about the uses of

those objects might be one such violation, generating a predictable response of "it's none of your business what web-sites I was surfing considering that I got the job done that I was assigned."

How surprising is it, then, that the information which is in those files, and which the government considers to be classified and top-secret, is viewed as the individual's right to dispose of as s/he sees fit? In many cases of espionage that dynamic can be seen as one of several motivating factors. Jonathon Pollard, for example, in addition to ideological motivations regarding his desire as a Jew to support the state of Israel, in discussing the information he sold rationalized his decisions regarding "his" files, which he knew more about than anybody else and was therefore most qualified to judge the need for secrecy. He did not steal files that were not in "his" territory until pushed to do so, and then experienced anxiety not present in previous acts of espionage. This pattern is typical of many spies, such as the Walker Ring, Craig Lonetree, and Klaus Fuchs.

The Ames case is particularly interesting because Ames did not for the most part follow this pattern. True, his first act of espionage did involve "his"files, but when he was shortly thereafter transferred to a different division (due to poor performance in his role at that point), he continued to acquire information from his previous position, but also other positions that he had no affiliation with.

If we accept Expectancy Violation Theory, then our notions regarding intellectual property become increasingly problematic. Intellectual property law was initially envisioned as a way to protect the original inventor or artist, by preventing duplication without proper permission. The notion of "selling" intellectual property rights was a novel adaptation under American law. Among the many details of government structure attended to by the founders of the Constitution, the establishment of the U.S. Patent Office might seem like a relatively minor insight. But by enabling the protection *and transfer* of intellectual property, the path to the current "information economy" became viable.

But exactly what kind of transaction is this transfer of intellectual property? Certainly, there is a legal status that is changed, a position called "ownership" that entails certain acts each party can and can't do. In almost every case, there is also a transfer of money. But what is getting exchanged in return for that money? The answer is... nothing. There is nothing, only an idea (which the philosophers have already concluded does not exist in any independent sense). The inventor/artist still has the same possession of the intellectual property that they always had, and as the individual most closely associated with the idea there is likely to remain a residual territoriality regarding it. The new owner also now shares that same idea, though perhaps not in the same way (and what is the legal status of an intellectual property right that I've sold but which the purchaser doesn't really understand, certainly not well enough to put the idea to use?), but it is a decidedly non-exclusive possession. There can never be a sense of primary territoriality.

Following this model suggests a communication-specific way of discouraging some espionage by eliminating the sense of ownership that enables secret-selling. Reducing the sense of ownership by ensuring that intelligence analysts do not work alone should improve the quality of the output, because the process of discussion should improve insights as well as reducing the sense of primary territoriality. Another possible way to reduce the sense of primary territory is to introduce a ritual to signify the passing of ownership, and to invoke such a ritual for every completed project rather than only once upon first hiring an employee.

Strategies Reducing Opportunities

An argument raised at the time of the Ames case, and particularly emphasized by Moynihan, is that perhaps intelligence does not need to be kept secret. Clearly, we still need to collect intelligence, but at the end of the Cold War it was not easy to see why that collection had to be clandestine or why the information resulting had to be kept classified. There is an argument to be made here: all those lives that Ames sacrificed need not have been lost if the CIA

refrained from insisting that its assets stay "in place," continue working for Russian agencies that they felt only ill-will towards. Let them defect to the U.S., openly and publicly, which most of the Russians had initially preferred to do anyway until the CIA pressured them into taking on the risks of continuing espionage. This was the preference of almost every Russian until the CIA pressured them into taking on the risks of continuing espionage. If they had defected, the information thus openly collected could be used more freely. This is part of the argument Ames himself made in a highly publicized fifteen-minute speech at his trial and sentencing.

The CIA also receives public accolades when a defector becomes known, especially a defector from a position which enables him or her to provide information useful for policy analysis. So the agency's preference to always keep its "assets" in place does not stem from lack of viable alternatives. Insisting that their new contact remain working in his original position is extremely dangerous for the Russian or Iraqi that offered his/her services. The need to maintain contact, including providing a plan for safe exit in case of emergency, requires that the CIA also place the lives of one or more of its own agents at risk. The potential danger is offset by the possibility of important new information coming to light, but this possibility is lower than the naive spy-novel reader might think for two reasons. One is that little changes for the average employee of any bureaucracy. To make the risk worthwhile, new information would need to arise within the two-to-five year period during which the would-be defector is usually able to remain in place before either giving up or giving himself away through changes in behavior, and before another asset is recruited. The probability of interesting new information is particularly low in organizations that are dedicated to secrecy and compartmentalize information routinely. The other reason the risk is less profitable is the difficulty of communicating with a source who cannot afford to take chances. Communication almost invariably has to wait until either an emergency, when the source leaves his or her country in a desperate escape, or until the source is trusted enough to be sent overseas. The clandestine meetings between trench-coat wearing

shadows that are so stereotypic of spy novels do not occur in territories ruled by oppressive regimes. Often, we do not hear a second time from a source that remains in place.

Strategies Relying on Organizational Culture

The benefit of a source-in-place, then, can only partially explain the CIA's insistence on assets remaining in place. The other part of the explanation has to do with the organizational values assigned to "assets" versus "agents." The "heroes" of the CIA have always been great "handlers," rather than the actual sources of information. In fact, the CIA has become rather well-known for failing to reward their assets. This privileging of agents over assets becomes clear when you read the rhetoric produced by and about spies within the agency. The FBI does not have a parallel relationship with its "informants." Perhaps this is in part because the FBI's informants are more likely to be criminals and less likely to be motivated by ideology. The FBI can afford to treat its information sources well because there is no danger that its employees will come to admire the individual. Admiration alters the relationship, and disguises the fact that the business they are in requires encouraging treachery. The FBI's sources are more likely to be motivated by fear of prosecution or a feeling of betrayal. By contrast, the CIA's "assets" are most often motivated by ideology, or sometimes greed. The CIA, like the KGB, also promises generous financial rewards, but it seldom follows through on those. Unlike the KGB, the CIA only rarely uses entrapment to blackmail anyone. The CIA's "assets" are also in some ways more crucial to the agency's mission than "informants" are for the FBI. The FBI often can and does prosecute cases without help from any informants. There are proponents of SIGINT at the CIA that argue electronic eavesdropping and satellite imagery are a substitute for HUMINT, but in general today and more so historically to collect intelligence meant only recruiting assets. So the differences between the two agencies in their treatment and valuing of individuals who betray their cohorts to assist the agency might seem contrary to what logic should dictate.

However, it is easier to understand the difference when you understand the crucial role

that this normative valuing plays. Specifically, the CIA MUST denigrate its assets, because there is no easy way to rhetorically distinguish between a Russian spy working for us and a CIA agent spying for the Russians. And for the CIA it is vital that a CIA mole be viewed as the most utterly despicable, incomprehensibly low traitor imaginable. The agency has relatively few obstacles to prevent its own trusted agents from engaging in espionage: only the ritual background checks prior to placement, and the relationships formed with coworkers. If the perception does not exist that to spy is the ultimate betrayal of your coworkers and you can be certain that they will hold you in contempt merely for the suspicion, then there is less of an obstacle preventing spying. The CIA does not and probably cannot so distrust the agents it gives classified access as to search every one of them on the way out every day, or to conduct frequent audits of their personal finances. This denigration of any individual engaged in treachery, to their own or to an enemy organization, is an additional strategy used to create greater trust within the agency and greater distancing from outsiders, to encourage the preservation of secrecy.

The greatest drawback to this strategy is the impact in a case like Ames. Ames is able to not see the humanity of those whom he betrays and sends to their deaths, because throughout the CIA those individuals get referred to with labels such as "assets" and manipulated with carefully taught and prized skills, a set of interpersonal strategies referred to as "handling." Outsiders who have not been enculturated into such language practices and behaviors react with horror at the apparent coldness with which spies have carried out their treachery. Ames is a clear example of this disconnect between the perception of an insider and that of the general public, which reacted with an initial outcry of revulsion. Only when we start to see intelligence work from the perspective of an insider do we begin to sense the wilderness of the maze of mirrors that leads to an outcome like the Ames case. His own words seem to summarize the case best.

> "The Great Game is rotten through and through. Spies spy on spies spying on spies, and none of it produces intelligence that those in power will ever use, or even want to hear. These spy wars are a sideshow, which have no real impact on

> our significant security interests over the years, carried out by careerist bureaucrats who have managed to deceive several generations of the American public about the necessity and the value of their work. ... The information our vast espionage network acquires at considerable human and ethical costs is generally insignificant or irrelevant to our policy makers' needs. Our espionage establishment differs hardly at all from many other Federal bureaucracies, having transformed itself into a self-serving interest group, immeasurably aided by secrecy."

But after the 9-11 attacks, in retrospect it becomes harder to make an argument that intelligence collection and secrecy are not both absolutely essential. So the tension remains, because it is also inevitably true that greater sharing of information creates greater likelihood of leaks, and a greater amount of classified information also by itself increases the likelihood of leaks.

"The investigation by the congressional committee led by Rep. Christopher Cox (R-Newport Beach) into unauthorized transfers of highly sensitive technology to China was so caught up in Washington's anti-China hysteria and was so influenced by Trulock that its conclusions cannot be trusted."--Michael Parks, director of School of Journalism for USC Annenberg and editor of Los Angeles Times between 1997 and 2000, published on MSNBC website Sunday March 31, 2002 titled "Paranoia Strikes Deep"

Wen Ho Lee and the Post-Cold-War Espionage Genre

The highest-profile[19] espionage case of recent years came to an astonishing end on September 13, 2000. Federal Judge Parker accepted a plea-bargain in which Wen Ho Lee agreed to plead guilty to one count of mishandling classified information, with a sentence less than the time he had already served in prison. Not only did Judge Parker end the two-year saga by accepting the plea bargain, Parker then proceeded to make headlines around the nation by apologizing to Lee, and criticizing the executive branch of the federal government.

..."Dr. Lee, I tell you with great sadness that I feel I was led astray last December by the executive branch of our government through its Department of Justice, by its Federal Bureau of Investigation and by its United States attorney for the district of New Mexico, who held the office at that time.

I am sad for you and your family because of the way in which you were kept in custody while you were presumed under the law to be innocent of the charges the executive branch brought against you.

I am sad that I was induced in December to order your detention, since by the terms of the plea agreement that frees you today without conditions, it becomes clear that the executive branch now concedes, or should concede, that it was not necessary to confine you last December or at any time before your trial.

I am sad because the resolution of this case drug on unnecessarily long. Before the executive branch obtained your indictment on the 59 charges last December, your attorney, Mr. Holscher, made a written offer to the office of the United States attorney to have you explain the missing tapes under polygraph examination."[excerpts from various trial documents deleted here]

"It is not only the top decision makers in the executive branch, especially the Department of Justice and the Department of Energy and locally, during

> December, who have caused embarrassment by the way this case began and was handled. They did not embarrass me alone. They have embarrassed our entire nation and each of us who is a citizen of it.
>
> I might say that I am also sad and troubled because I do not know the real reasons why the executive branch has done all of this. We will not learn why because the plea agreement shields the executive branch from disclosing a lot of information that it was under order to produce that might have supplied the answer.
>
> Although, as I indicated, I have no authority to speak on behalf of the executive branch, the president, the vice president, the attorney general, or the secretary of the Department of Energy, as a member of the third branch of the United States Government, the judiciary, the United States courts, I sincerely apologize to you, Dr. Lee, for the unfair manner you were held in custody by the executive branch." –Judge Parker's Wednesday, September 13, 2000 statement upon accepting the plea-bargain arrangement.

Judge Parker's apology was echoed by President Clinton the following day at a news conference[20]. The highest-profile espionage case ended by becoming one of the highest-profile errors of the Federal Bureau of Investigation, an agency which at that time had already come under heavy criticism[21]. How did the case of Wen Ho Lee ever get to a point where such apologies were felt to be appropriate? If the evidence in the Wen Ho Lee case was so weak that it was seen as "an embarrassment," then how did it become such a high-profile espionage case?

To understand the case of Wen Ho Lee, it is necessary to understand the rhetorical situation in which the case emerged. Or rather, it becomes necessary to understand the series of overlapping situations which resulted in the Lee case, which emerged as an almost fore-ordained necessary closure. The lack of sufficient evidence to support the initial charges against Lee was sufficient to generate a high-profile espionage case because of the initial expectations set up by the Cox Report, because of the expectations regarding repressed evidence inherent to espionage narratives, and because of the internal dynamics of press coverage and inter-agency relations.

The espionage investigation which ended with the judge's apology began in 1995. Two separate events occurred, each of which could be considered the "beginning" of the Lee case.

One event was the realization that China had successfully tested a "miniaturized" nuclear warhead. The other event was a media-and-criminal investigation into technology transfers from U.S. satellite companies to the Chinese. These two beginning points converged by 1997 into a heightened fear of Chinese espionage, which combined with a political context in which our relations with China were worsening already.

Event One: China's Miniaturization Success

The conclusion that China had succeeded with a miniaturized nuclear warhead had been in the works since 1992. Shortly afterwards (1994) the Chinese signed the Nuclear Test Ban Treaty. The analysis which eventually drew this conclusion was highly secret, so there was little or no public alarm about it at that time. In secret, however, the analysts at NN30, which is DOE's counterintelligence unit, were drawing together evidence that later would set off alarm bells. The evidence was all highly classified, drawn from U.S. spy satellite images, seismic data, and eventually (1995) word from a Chinese informant who confirmed that indeed the 1992 test was a miniaturized weapon and indeed it had been successful. In retrospect, this should come as no surprise: the Chinese had known it was possible and been working towards this goal since the beginning of their nuclear program, and numerous questions they had asked and presentations they had given (including a public speech at LANL by their third-highest ranking official in their nuclear program back in 1986) indicated that they had known the basic secret was to create an asymmetrical bomb, rather than a spherical bomb. Of course, knowing it would happen eventually and realizing that it had already happened are quite different matters emotionally. The individual in charge of NN-30 was Notra Trulock, an intelligence analyst who had begun his career studying the Russians, and the Russians had needed more than a dozen tests before succeeding with miniaturization. Upon reading the report that the Chinese had succeeded with their very first test of a miniaturized weapon, his immediate conclusion was that the only way this could have been possible was espionage. And following the usual (Russian) model of

atomic espionage, that meant there was one very well-placed spy who had access to top-secret weapons development information.

The observer might initially be struck by the conjunction of those two sentences. There is something of a non-sequitur at first reading. Nevertheless, the lessons of history in all the cases of atomic espionage, and indeed most of the best-known espionage cases, suggest that the assumptions necessarily went together: historically, if there has been espionage of highly-classified weapons information, then there is a single well-placed spy supported by a network of agents who are involved in the conspiracy but are not themselves able to access the information to be stolen.

The number of atomic espionage cases in U.S. history is very limited, so for the record here I will survey the entire list, in order to illustrate that while Trulock's reasoning was flawed, his assumptions were not wholly irrational. His reasoning was that of any expert deeply versed in the dominant views of his area of expertise.

The History of Atomic Espionage

There were at least three spies at Los Alamos during the Manhattan Project, and other research sites were also penetrated by secret agents. For example, cross-sectional data was still being collected at the University of Chicago, and plutonium production was being done at Oakridge Tennessee, and Uranium mining and refining was being done in Canada. Russian spies were in place at all of these facilities–John Hiskey in Chicago at Compton's lab, Alfred Slack at Oakridge, and Bruce Pontecorvo in Canada.

The most famous of the atomic spies was undoubtedly Klaus Fuchs[22], later placed in charge of Britain's nuclear weapons program at Harwell. Fuchs was a member of the official British delegation; as such his security clearance was vouched for by the British and the U.S. Army (uncharacteristically) accepted their vouchsafing. But in fact Fuchs had only received British citizenship after he fled Nazi Germany, and his Communist ties had already been

established, and were in fact known prior to his admission to citizenship. The prevailing view was that this made him a more reliable enemy of the Nazis, and thus he could be trusted with secret weapons research. But Fuchs began passing information to the Russians even before he left Britain. He primarily passed them information about his own work, the separation of Uranium isotopes, but also some general information about the project. After his Christmas holiday, the Russians arranged for a courier named Harry Gold to meet him occasionally in Santa Fe. Though only a very preliminary investigation by the British had been begun, based on tips from the FBI that they considered unreliable, in 1949 Fuchs confessed voluntarily and was sentenced to a short prison term. Because Russia had not in fact been Britain's enemy during the war, Fuchs could not be tried for treason or any more serious charges, and his light sentence rankled the Americans. After serving nine years in prison, Fuchs moved to East Germany and headed a research lab there. Fuchs is a particularly controversial spy, because he turned himself in rather than an investigation "catching" him, and because of his light penalty, and because of the timing of his conviction. Specifically, Fuchs' arrest was announced mere days after Eisenhower announced that he would push forward research on the Hydrogen bomb, and that research was considered more urgent because it was believed by some that he might have given the Russians secret information on early discussions regarding the Hydrogen bomb. This issue has since then been fairly convincingly disproven by scientists[23] noting that a) the state of speculation regarding the Hydrogen bomb at the time Fuchs might have had access was so completely wrong that it would have hurt rather than helped Russian researchers and b) the speed of the Russian's acquisition of hydrogen bomb capability can be better explained by realizing that the tests on Bikini Island would have made most of the relevant information available to anyone interested and capable of collecting the data afterwards.

The youngest Manhattan Project spy was Ted Hall, who was only 19 when he began spying for the Russians. Like Fuchs, Hall spied for ideological reasons. Whereas Fuchs gave

secrets to the Russians because he was a life-long Communist, Hall gave secrets to the Russians because he did not want the U.S. to be the only government in possession of the atomic bomb, for fear that it would become too powerful. Hall provided information on the general layout and personnel at Los Alamos, and further information particularly regarding his own work on the shaping of the charges, or the "lenses," for detonation. Hall left the country after the war, thus escaping the possibility of criminal prosecution.

David Greenglass, the only Manhattan Project spy prosecuted in the U.S., was a member of the Army rather than a member of the scientific staff. Greenglass was a machinist who had been trained in handling metals that are difficult to work. He had little understanding of what the secrets he sold to the Russians were designed to do. Primarily, Greenglass was useful for confirming that Fuchs and Hall were genuine and not "plants," and for his attempts to recruit other spies from among the Los Alamos personnel. His brother-in-law, Julius Rosenberg, was a "spy-master" who served as courier and task-master for a ring of 10 or so spies working in a variety of industrial positions, and whose most useful theft was an electronic fuse.

The "atom spies" became known for two reasons: Fuchs' voluntary confession, and the NSA's[24] decryption of the Soviets' wartime codes, a project code-named Venona. The Venona project was kept extremely secret, not shared with the British MI6 or the FBI or even the U.S. president or Congress. The secrecy of the Venona Project was guarded so carefully that the officials responsible refused to allow any knowledge of the project to be used in prosecuting the atom spies, even though the decrypted messages were the original source of our knowledge[25]. So prosecution of the U.S. atom spies relied entirely on what today we would call circumstantial evidence and the testimony of Harry Gold (the courier for Fuchs and Greenglass), because the key evidence (i.e., the decrypted tapes of the Soviet transmissions) was judged more valuable secret than used in the prosecutions. In 1994 Senator Patrick Moynihan successfully argued that crucial historical information, such as the Venona Project, needed to be declassified. The

declassification was matched by the Russians, who opened many of the files of the former-KGB regarding these atomic spies. The declassifications resulted in renewed interest and greater understanding. Because of the mutual declassification, it is reasonably certain that we know all of the cases of atomic espionage. And because they are so thoroughly known, it is easy to see the patterns across the cases and draw conclusions based on this which have no easy counter-examples. The cases suggest that nuclear spies are more likely to be ideologically motivated than financially motivated, are likely to be relatively highly-placed sources who betray many secrets rather than simply one or two that are easily available to them, and that espionage is centrally controlled by a powerful foreign enemy. The history of nuclear espionage provides a pattern that both guides counterintelligence work and hinders counterintelligence work, when a case fails to fit the historic pattern.

Event Two: Satellite Technology Transfers

The November 1994 Congressional elections resulted in the installation of a newly Republican majority. The Democratic presidential administration almost immediately came into conflict with the new Congressional majority. Conflicts about homosexuals in the military and health care policy reforms heightened the ideological rift between parties during the following years. In 1996, the Republicans accused Clinton of accepting campaign finances from Chinese citizens, and in return compromising American national security interests in regard to China. One example cited was the increase in exchange programs between Chinese nuclear scientists and American nuclear labs. Another example cited referred to a New York Times reporter who had revealed that two American companies, Loral and Hughes, while diagnosing the reasons for the many launch-failures of the

Chinese satellite program had revealed classified information during their consulting.

This author, Jeff Gerth, in 1995 did a piece of investigative journalism revealing that one of the U.S. satellite companies, contracted by the Chinese government to help diagnose the cause of why their space shuttles were failing, had given away technological secrets used by the defense industry to improve ICBM launching. Space and military research being so closely related, these technologies are classified as "dual-use" technologies. All dual-use technologies are carefully controlled as to when and to whom they can be exported. Any export of the procedures for launch-diagnosis is regulated by the EAR (Export Administration Regulations) and therefore must be approved (or not approved) by the State Department. The company, Hughes[26], did not follow the approval process, and amidst the accusations regarding Clinton's dealings with China, this led to Congressional hearings.

Not coincidentally, Jeff Gerth became the primary reporter initially assigned by the New York Times to the Wen Ho Lee case when it became public. Gerth is a Pulitzer-Prize winning journalist. His coverage of the Lee case, however, came under heavy criticism, and he was eventually removed from the story by the Times' editors. In a retrospective review of the media coverage of the Lee case, Michael Parks, director of School of Journalism for USC Annenberg and former editor of the Los Angeles Times, stated:

> The news media fanned this Sinophobia. Fed by Trulock and other federal officials motivated by self-interest, *New York Times* investigative reporters Jeff Gerth and James Risen raised the alarm about the supposed theft of the country's 'crown jewels' and compared the case to that of the Rosenbergs. Knowledgeable specialists in the paper's own newsroom, however, should have quickly exposed the many holes in the case, and its editors should have questioned the bias of the sources. In fact, six months later, William Broad, a *Times*' science writer with much experience reporting on nuclear armaments, interviewed physicists and weapons specialists at Los Alamos for another major piece and concluded that there was strong disagreement about how much help China had received, or needed, to advance its nuclear arsenal. However, the *Times*' two re-examinations of the case were, in the view of Stober and Hoffman, largely self-exculpatory,

> trying not to admit any failure on the paper's part while setting the record straight.
>
> But *The New York Times'* first story, the 3,800-word account by Gerth and Risen of the investigation at Los Alamos, set other news organizations in pursuit of the agents that China allegedly had within the U.S. weapons establishment. As editor of the *Los Angeles Times* through most of this period, I pressed our reporters to catch up with *The New York Times*, but they came back highly skeptical of the Cox report and of the case against Lee. Columnist Robert Scheer, based on his own reporting, argued on this newspaper's Commentary page that Lee was a victim of racism and the case against him was fatally flawed.
>
> Investigative reporting is an important defense of American democracy, but in the case of Wen Ho Lee, it contributed to the fear-mongering political atmosphere in Washington and nearly subverted justice. First Amendment rights imply the obligations to be factual and accurate, truthful and fair and, in my view, compassionate as well. As a profession, we failed this test in the Lee case and consequently diminished the credibility of investigative journalism." --Michael Parks, published on MSNBC website Sunday March 31, 2002 titled "Paranoia Strikes Deep"

The review by Parks is highly critical of the media coverage of Lee, and avoids an "I-told-you-so" tone only because he himself admits to having pushed his journalists just as hard. The more interesting point to be gleaned from this criticism of media coverage, however, is the awareness that the media discourse is driving the discourses of those inside the intelligence communities and the legal community. Responsibility is placed on the media through the use of verbs like "set" and "based on his own reporting." This assignment of responsibility is echoed in accounts by community insiders as well. Trulock comments that the NYTimes coverage "lit a fire" under the FBI investigators, and led to the first polygraph of Lee. Similarly, media discourses are intertwined at every stage of the espionage case.

ENTER THE COX REPORT

The Congressional hearings were designed to investigate not only Hughes' and Loral's possibly illegal communication, but the extent to which the Chinese had stolen other technological secrets. Their mission statement was published in the Appendix attached to their report as follows:

> "Pursuant to House Resolution 463, the Select Committee was authorized

> to investigate a broad range of issues in relation to the transfer of U.S. technology to the People's Republic of China. Among other things, the responsibility to investigate any transfers that may have contributed to the enhancement of the accuracy, reliability or capability of the PRC's nuclear-armed ICBMs or other weapons, to the manufacture of weapons of mass destruction, missiles, or other weapons, or to the enhancement of the PRC's intelligence capabilities." (Appendix A)

The bipartisan committee consisted of five Republicans and four Democrats, and was chaired by Congressman Robert Cox (R-CA). The climate for the committee's investigation was strongly influenced by the 1996 scandal regarding Chinese donations to Clinton's campaign (at the same time Vice President Gore was criticized for his fund-raising at a Buddhist temple). This committee came to be called the Cox Committee, and their conclusions were released first as a classified report (January 1999), and later (May 1999) an unclassified version of their report. The committee's investigation grew from initially disparate events, such as the two previously discussed, and also a series of events that created a worsening of tensions between the U.S. and China. Elections in Taiwan, the mistaken bombing of the Chinese embassy in Belgrade by the U.S., and the furor over the president's fund-raising all contributed to a political climate in which the Cox Committee released its report, in which China was positioned increasingly as a potential enemy of the U.S.. The Cox Report in turn raised the profile of the Lee investigation and strongly influenced the process of the investigation and eventual trial.

The Cox Report is the short name for the Report of the Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China, chaired by Senator R. Cox (R-CA). The Report starkly claims that "The People's Republic of China has stolen design information on the United States' most advanced thermonuclear weapons." (p. 1) For the next 368 pages (in the declassified version), that claim is magnified and elaborated. After the initial release of the report, the committee members continued activities that have kept national security and secrecy issues highly visible. For example, former Senator

Rudman (R-NH) repeatedly argued for the restructuring of the Department of Energy (DOE), which is responsible for oversight of our two national weapons laboratories, along with many other energy-related research and administration projects), based largely on claims made in the Cox Report and follow-up investigations.

The Cox Report is vital to consider here because it sets the stage for the Wen Ho Lee case. The Cox Report is of interest more generally because of the ways in which it functions rhetorically. The Cox Report is fundamentally about secrets and violations of secrecy. In order to work effectively around the silences that are a necessary result of talking about secrecy, the Cox Report employs three primary strategies. It relies heavily on pathos, creating a mood of alarm in the audience. It relies upon ethos, in the form of claims of authority that highlight the committee's access to secrets that the audience has no access to. Finally, the report relies upon audience expectations that are built up from familiarity with previous texts regarding espionage, texts which would guide the audience in a specific reading strategy and would influence the role of evidence. These three strategies enabled the Cox Report to have had significant impact on the public discussion of the Lee case as it developed, in spite of the fact that the Report itself was criticized regarding numerous faults and in numerous forums almost as soon as it was published.

Most of the reactions to the Cox Report were driven by politics, rather than by the content of the report itself. Conservative groups largely accepted the conclusions, sometimes using the Cox Report as the basis for labeling Clinton "treasonous." Democrats were largely silent.

The reaction among Asian media, and foreign media generally, dismissed the Cox Report as propaganda. The official response of the Chinese government on July 15, 1999 concluded, "Voluminous facts indicate that the essence of this report is to fan anti-China feeling and undermine Sino-US relations. To achieve this political purpose, the report leaves no stone unturned to distort facts, substitute one thing for another, make subjective assumptions and

groundless accusations and resort to demagoguery. The conclusions of the report, therefore, are utterly absurd and do not hold water." (from "Facts Speak Louder Than Words and Lies Will Collapse by Themselves")

Other criticisms were based on the content of the Report. For example, a few months (December 1999) after the release of the Cox Report, the Center for International Security and Cooperation at Stanford University published an assessment of the Cox Report which criticized it fairly extensively. The five co-authors of the assessment criticize the Cox Report's for misrepresenting China's political structure, policies, nuclear capabilities, and ability to steal or use stolen information. The assessment points to places where quotes were taken out of context (one of the authors quoted, Iris Chang, made presentations at numerous Asian Studies conferences specifically denouncing the ways in which her work was used in the Report), statements were incorrectly attributed (for example, a claim which in the footnotes is supposedly supported by reference to the PRC Constitution, but when checked the source has nothing to do with the claim being made), and factual errors were included (such as listing the Chinese missiles' range in terms of miles instead of kilometers without doing the numeric conversion, thus greatly exaggerating their danger to U.S.). The introduction to the assessment concludes, "In short, the discussion of Chinese politics, economic modernization, and nuclear doctrine lacks scholarly rigor, and exhibits too many examples of sloppy research, factual errors, and weakly justified inferences." (p. 11) The authors point out that they were working from the declassified version when they wrote the 104-page assessment. The assessment is largely a list of specific errors made in the report compiled by each author in their own area of specialization. The authors point out in the conclusion, "The surprising number of technical and numerical errors, and the occurrence of selective one-sided quotations from publicly available books and references noted by many reviewers, are such that the quotes from sources not publicly available should be considered suspect as well." (p 97)

Given that the reactions to the Cox Report were largely political, the style of the Report might seem to be less significant. Nevertheless, as rhetoricians sensitive to the power of word choice and other stylistic matters, it is worth spending some time analyzing the Cox Report. In addition to its interest as precursor to the Wen Ho Le case, the Cox Report is of interest in terms of rhetorical theory because the publicly available version provides a new way of thinking about silences and taboos. Usually when rhetorical theorists write about "the unspeakable" and about "discursive absences," we are writing about topics that are off-limits for normative, cultural reasons (sexual taboos, the voices of the powerless, etc.). In this case, however, the "unspeakables" are explicitly imposed by government censors, and the discursive absences are precisely those which previously functioned as the evidence and supporting examples that backed up the strong claims made in the Report. The holes left behind in the body of the argument create a rhetorical exigence of an unusual sort. How can an argument be persuasive when the heart of the argument–the evidence supporting it–cannot be presented? What rhetorical strategies are available that can circumlocute the necessary silences and still be effective? There is a challenge here for both the rhetor and the rhetorical critic: the rhetor cannot fill in the discursive absences, even if the government censors would allow them to, because to give away national secrets in the same document complaining about theft of our national secrets would be counterproductive. The critic is asked to interpret and analyze a document in which the most critical pieces are missing, like a jigsaw puzzle where you don't have the original picture and not all the pieces are still in the box.

Appeals to Pathos

As stated before, one of the strategies used is a reliance on pathos. The result was a tone which can be summarized in a single word: alarmist. For example, the introduction by former Secretary of Defense Caspar Weinberger, states:

> "Many important aspects of the Report remain secret, as they should, in the interests of national security. But enough has been made public now, after long delays and blocking actions by the Clinton-Gore administration, to let every American know that what the Cox Report has uncovered regarding espionage by agents of the PRC is the most serious breach of national security since Julius and Ethel Rosenberg betrayed our atomic secrets to the Soviet Union and Aldrich Ames sold us out for a mess of pottage. For their crime, the Rosenbergs were executed. The crimes uncovered here by this Report have yet to be redressed." (p. vii)

This is a rather telling way to end the introduction, given that there is still some question regarding whether both Rosenbergs were guilty of selling out any atomic secrets. The parallel established here in the introduction to the Cox Report becomes particularly significant after the Lee case becomes public knowledge, because this parallel is treated as a threat. The New York Times' first story about Wen Ho Lee paraphrases Weinberger, with the implication that Lee should also be executed, as the Rosenbergs were. During the FBI interrogation of Lee, this threat is brought up again by agent Carol Covert in an attempt to make Lee confess.

The first chapter of the Cox Report, after some introductory comments, begins with a large-font, shaded box stating, "The People's Republic of China (PRC) has stolen classified design information on the United States' most advanced thermonuclear weapons. These thefts of nuclear secrets from our national weapons laboratories enabled the PRC to design, develop, and successfully test modern strategic nuclear weapons sooner than would otherwise have been possible. The stolen U.S. nuclear secrets give the PRC design information on thermonuclear weapons *on a par with our own*." (p. 1) (italics mine) At other points in the same Report the committee backpedals away from this claim, as on p. 8 where it declares (in a smaller font and in the middle of a paragraph), "Although the United States has been the victim of systematic espionage successfully targeted against our most advanced nuclear weapons designs–and although the Select Committee judges that the PRC will exploit elements of those designs for its new generation of ICBMs–the United States retains an *overwhelming* qualitative and quantitative

advantage in deployed strategic nuclear forces." (italics mine) This second statement is directly contradictory to the opening statement, and is much closer to the truth. Within the text of the Cox Report, neither assertion is supported. The contradiction tells us both something of the Cox Committee's goal and something of who the Cox Committee believed their audience to be. The more prominent claim has the effect of exaggerating the danger to the U.S., but the claim can only work for a general audience, not an audience of defense experts. An audience already familiar with defense policy would almost certainly be aware of the numbers behind the claim of "overwhelming advantage:" for example, the U.S. has 17,500 nuclear warheads and the PRC is estimated to have only 400, of which only about two dozen are ICBMs. These numbers are publicly available–my source here is from a 1999 Military Almanac, but various web-sites and numerous government documents contain very similar statistics.

In almost every other place in the Cox Report, the use of the past tense ("enabled") is replaced by the use of the future tense, as in headings such as "the Select Committee judges that elements of the stolen information *will assist* the PRC in building its *next* generation of mobile ICBMs, which *might* be tested this year," (p. 6, italics mine) and "The introduction of small warheads into PLA [People's Liberation Army] service could coincide with the initial operational capability of the DF-31, which *could be ready* for deployment in 2002." (p. 7) Thus, the Report puts forth strong, alarming-sounding claims phrased in the present or past tense, in the bold headlines. The Report then backs off from the claims, using future-conditional tense verbs and other hedge-words, but the clarification is in a much smaller font which only the truly dedicated will bother to read. Thus the Report manages to stake its claim to the more extremist ground without having to properly defend it.

Another appeal to pathos is in the Report's use of visual rhetoric. For example, on page 99, there is a full-page image of the mushroom cloud resulting from a nuclear explosion, superimposed by the words "The PRC has stolen classified information on every currently

deployed thermonuclear warhead in the U.S. ICBM arsenal." The use of repetition emphasizes the exaggerated claim and reinforces it with the use of striking photographic imagery.

Another way in which the Report creates a feeling of alarm is the way in which future-conditionals are strung together. For example, a bold headline on page 172 declares "The PRC's new mobile intercontinental ballistic missiles, and its planned new submarine-launched intercontinental ballistic missiles, will use smaller warheads." A chart on the opposite page provides approximate distances to selected target cities in the U.S. and Europe within range of where silos are reportedly located in China. The overall impression at first glance is that China has built new missiles with stolen U.S. technology that can blow up the list of cities. Upon reading through the smaller print of the text itself, however, a different point is actually being made. The text states:

> "Because U.S. thermonuclear warheads are significantly smaller, they are capable of use on mobile missiles and submarine-launched missiles. The Select Committee judges that the PRC will attempt to steal and exploit elements of U.S. thermonuclear warhead design information to build their new ICBMs. If any of the PRC's planned missiles were to carry multiple warheads, or if the CSS-4 [China's current model of ICBM] were modified to carry multiple warheads, then a fairing [a covering for the missiles in the nose cone, said to be similar to the problem Hughes had helped diagnose regarding PRC satellites] could be required. The aggressive development of a MIRV system by the PRC could permit the deployment of upwards of 1000 thermonuclear warheads on ICBMs by 2015. Three new ICBMs are reportedly being developed by the PRC. ... The DF-31's 5000 mile [actually kilometer] range could allow it to hit all of Hawaii and Alaska and parts of the state of Washington. The DF-31 could be ready to be test this year. Given a successful flight program, the DF-31 could be ready for deployment as early as 2002."

Note that there are eight conditionals in this statement, and each depends on the preceding conditional being satisfied. There are a lot of "if's" between the premise and the conclusion. At no point does the Report provide evidence to increase the likelihood of any of the conditionals. Why would the PRC suddenly multiply their ICBM arsenal by more than forty times its current

size? The Cox Report provides no answer, gives no indication that China intends to, and merely asserts that they "could." The problem is compounded by the Report's frequent use of this strategy.

Appeals to Ethos

The need to present an argument in which the evidence itself is declared secret, rather than being downplayed, is highlighted through the use of references to self-censorship and at other times to administrative censorship that pervade the Report. For example, in the first chapter alone, which is only 34 pages, there are seven instances where the Report specifically draws attention to government censorship, with statements such as "IMPORTANT NOTE: This declassified report summarizes many important findings and judgements contained in the Select Committee's classified Report, issued January 3, 1999. U.S. intelligence and law enforcement agencies within the Clinton administration have determined that other significant findings and judgements contained in the Select Committee's classified Report cannot be publicly disclosed without affecting national security or ongoing criminal investigations." (p. 1, shaded box at top of page) In numerous other cases (averaging roughly every five paragraphs), rather than explicitly referring to the censorship process, the Report uses language such as "the Select Committee judges that..." with no further supporting evidence. This phrasing hearkens back to the explicit statements about censorship. The reader might well assume that the *classified* version must surely contain a great deal of supporting evidence, since there are so many points at which its discursive absence is highlighted.

Through the references to censorship, the use of passive voice, indirect language, and other circumlocutions, the Cox Report creates a fog of mystery. This linguistic fog is the strongest claim the Report has to be called "artistic." Of course, much bureaucratic rhetoric consists of linguistic fog (Shuy, 1998), but in the case of the Cox Report the approach is strikingly parallel to the ways in which fictional spy novel mystery writers develop suspense,

and tantalize the reader with clues that they might catch if they read carefully. The Report is not clear, it does not even try to make itself clear. The reader is left with silences that are set in a context in which those very silences are meant to be the primary mode of signification. The silences justify claims without need of evidence or concrete reasons. As Ehrenhaus notes in his article on "Symbolic Uses of Silence," silence speaks, and allows the listener to hear in that silence whatever s/he is able or wants to hear. The Cox Report is taking advantage of that in order to construct spaces that the reader is left to fill in.

Audience Expectations

To further function persuasively, the Report uses the form of a spy-thriller novel. Like a spy novel, the Cox Report is most persuasive for an audience which assumes that the mechanisms leading to a public disclosure are more complex (more nefarious) than a surface-reading would indicate. And this inclination towards a hermeneutic of suspicion provides rewards when applied to the text and context of the Cox Report.

In understanding the Cox Report's effect, I appeal to Burke's notion of form. In Burke's sense, "form" is the creation of an expectation in an audience, and then the satisfaction of this expectation, although the violation of the expectation has its own effect. The persuasive use of form, then, depends upon being able to establish expectation. One way to do so is to demonstrate a pattern internal to the text. Examples might include the use of linguistic forms such as anaphora ("I knew Jack Kennedy. I worked with Jack Kennedy. And you, sir, are no Jack Kennedy!") or scala ("He who controls Berlin controls Germany, and he who controls Germany controls Europe. He who controls Europe controls the world, and therefore we must not allow the Russians control of Berlin"), in which a part of a sentence gets repeated or repeated with variation. This establishing of

an internal pattern can be done on a larger scale as well, as the organizing principle for an entire text. Another possibility is the use of a pattern developed elsewhere, external to the text, which the persuasive text can then draw upon to create an expectation in the audience. This is one of the effects of genres. The audience develops an expectation for how a text is going to proceed and derives satisfaction from participating with the text in its unfolding.

This use of form is culturally bound. If the audience does not already recognize the pattern from somewhere, the text alone will not function as persuasively. The expectations are not somehow biologically built into us, except perhaps extremely elementary ones[27]. In arguing that the Cox Report draws heavily on the use of form in order to achieve its persuasion, one must first establish what the expectations aroused would be, and where that form comes from. At an elementary level, perhaps, the form that it follows might be common enough not to need much work to establish: if there has been a wrong done, there needs to be a villain. So the set-up demands a scapegoat, which lays the groundwork for the Wen-Ho Lee case. The expectation is based on form at such a basic level that it would be difficult for any western audience to avoid the expectation. But my argument regarding the use of form goes further, because I mean to argue that the Cox Report is designed for an audience that will read the evidence presented, and the evidence not presented, in a very specific way. And that way of reading evidence, and of looking "between the lines" for hidden evidence, that might provide further clues as to how events will unfold, is an expectation that audiences develop from reading mystery novels or watching films, whether of the crime-solving genre or of the spy-thriller genre. Insofar as the Cox Report follows the patterns of one genre, audiences familiar with that genre will be further persuaded by its use of form.

The following paragraphs on this topic of spy-thrillers fit in to establish the expectations of the genre, and from there to demonstrating that the Cox Report follows that same form. Maybe the Paranoid Style is sufficient to explain the persuasiveness of the Report[28], in that the

expectations are derived from and available in many places in American culture. Perhaps conspiracy theories are widespread enough in America that even those who do not participate in the usual conspiracy-group forums are already halfway persuaded that the world is run by shadowy, secretive groups operating behind the scenes, and that therefore evidence of large-scale espionage is merely confirmation rather than outright persuasion. But the specific parallels between the Cox Report and the literary genre are also interesting. The committee's choice to make it publicly available as a book rather than through interviews on televisions, links on the internet, or late-night radio talk shows (which are the usual sources and forums for most conspiracy theorists) suggests that the use of the spy-thriller form is an important component of the Report's persuasiveness, and also tells us that the audience the committee was looking for would be one familiar with this genre.

Like the Cox Report, spy-thriller novels are a product of the modern age, developing only during World War I and not stabilizing or becoming popular until the Cold War. "That fears of imperial decline and national weakness provide an especially fertile breeding ground for spy novelists is amply proven if we look at the United States and the recent increase in the number, popularity, and output of American spy writers," notes Stafford (p. 215), in discussing the social contexts that are conducive to the genre. "The spy, compositely, in modern fiction signifies a man in an impalpable world of shadows, one who fears to express his genuine feelings, whose work cannot be discussed with others, and the precise nature of which he may himself be unaware. .... The spy's organization is narrowly and tightly compartmentalized, fostering clandestinity, and the agent may not be aware of his co-worker's real purposes or intentions." (Cawelti & Rosenberg, 1987, p. 211). This description of the literary genre of espionage novels is parallel to the argumentative structure and the position of the target audience for the Cox Report. In the Cox Report, the highlighted silences and references to material "the Clinton

administration deems unreleasable at this time," implies that there is a political (and Democratic) conspiracy that is behind the leaking of secrets. But no individual or group gets explicitly blamed. In spy novels, the audience participates by searching for clues as they read that will reveal "whodunit." Similarly, an audience reading the Cox Report is invited to search for clues, to follow the long chains of conditional reasoning to figure out for themselves "whodunit," who would have motive and opportunity. And in the end of the Cox Report, nobody gets blamed. The causes explicitly blamed for the loss of secrets include compartmentalization ("The Commerce Department decontrolled Garrett jet engines without consulting either the Defense Department or the State Department..." p. 30), the lack of knowledge of the activities of others ("In light of the vast number of interactions taking place between PRC and U.S. citizens and organizations over the last decade as trade and other forms of cooperation have bloomed..." p. 36), and the lack of communication between the various parties involved ("The President did not learn about the issue of successful PRC espionage at the U.S. national weapons laboratories and long-term counterintelligence problems at DOE..."p. 125). These characteristics are the same that Cawelti and Rosenberg note are the predominant world-shaping forces in espionage novels. The world that is portrayed in the Cox Report resembles the (fictional?) world that spy novelists create. The parallel between politics and art reinforces the persuasiveness of the Report: it can evade the need for a clear narrative form because the narrative for an espionage story is so well-known and it really is a stock set. Umberto Eco, for example, notes that the pleasure derived from James Bond novels (which are about as formulaic and predictable as any writing ever has been) consists in the fact that the reader "knows the pieces, the rules, and the moves, and watches it unfold, taking pleasure in the game and its minor variations."

John Snyder argued, in "The Spy Story as Modern Tragedy," that the relationship between man and government as seen in espionage novels (a uniquely modern genre) is tragic in its essence. As in Oedipus Rex, the individual must always be sacrificed for the good of the

state, and the bureaucracy of the state is manipulative and unscrupulously deceptive. The Paranoid Style, indeed, lends itself to a worldview that has more in common with tragedy than comedy. Belief in conspiracy requires an interpretation of events as sinister and significant, and the vigilance needed to avoid being manipulated demands a constant looking beneath the surface and assumption of dishonesty on the part of others. As with Classical tragedy, in which the will of the gods was the unpredictable and inevitable mover of events, in the modern Paranoid Style the machinations of government (or the secret powers behind the state bureaucracy) are unpredictable (because individuals cannot understand that which is carefully hidden) and inevitable, with layers upon layers of secrecy and manipulation entrapping the individual (even the individual spy working in service of the government). This layering makes possible the twists and turns of plot line in a typical spy novel. This layering also creates a relationship between man and state that is alienating and disempowering. Man's quests for freedom, rationality, and justice are hubris, doomed to disappointment and a tragic ending, according to the shared logic of the Paranoid Style and the generic spy novel.

In point of fact, however, the post-Cold War spy story seems to be more an example of comedy than of tragedy[29]. This was perhaps predictable. Writing in 1988, Ed Black noted that "The disclosure of secret agents and agencies is not terminal; it concludes nothing beyond itself. It is ad hoc, a transient skirmish in a prolonged conflict; it functions merely to confirm the ideological position that generated it. Such a disclosure is, in sum, not purgative. It leaves the fundamental affliction in place and extirpates only one of its local manifestations." (p. 60 in Rhetorical Questions) The crucial key to understanding tragedy is the moment of catharsis, which alone can signify the necessary closure. In espionage, there is no moment at which everything becomes clear and all the secrets are revealed. For the paranoid, there is always the suspicion that where there was one double-agent, there might be more who are better hidden. For the individual onlookers, there is always the suspicion that what the state bureaucracy (CIA,

FBI, or KGB, it doesn't matter) is not revealing is greater than what is revealed by the limited disclosure of the spy case, and that context might very well alter our understanding of the case at hand.

Burke's notion of "form" suggests that a rhetorical text sets up certain expectations in its readers/listeners, and that the audience receives satisfaction when those expectations are fulfilled. The audience is persuaded by the rhetoric insofar as it is caught up in the expectations created by the form, and then satisfied. My claim, then, that the Cox Report functions in this way rests on the assumption that the audience to which it is directed would be familiar with the form of mystery/spy fiction. What does this say about who that audience is? Not politicians, at least not in particular–though presumably the longer, uncensored version of the Report is not immensely different in form, and that is the version the relevant politicians would be presented with. The usual audience for mystery/spy novels consists of somewhat educated, but disaffected readers–they are widely popular, a staple of the conservative conspiracy-theory types and simultaneously of college-educated workers in bureaucratic posts. (Cawelti, 1987)

It is entirely possible that the cause-effect arrow points in the opposite direction from what I've implied above–mystery/spy writers (who truly do place a premium on trying to be realistic, as Stafford notes) write the way they do because that is what in fact must emerge from a national security bureaucracy dealing with the public. Through the course of the Cox Committee's investigation of Chinese espionage, increased attention and investigation was stimulated, and that in turn brought to light new information about potential leaks: specifically, the scandal surrounding Wen-Ho Lee. The Lee scandal was crucially influenced by, and in fact I would argue received such high media visibility primarily because of, the rhetorical situation which the Cox Report created.

One of the other abiding characteristics of the espionage genre: there is usually a hero (though particularly in early examples of the genre that hero tends to be flat and one-

dimensional), but there is always a villain, and one of the characteristics of the genre (as distinct from any other type of adventure or thriller novel) is the importance of developing the nature of the villain (Handberg, 1991). So, to follow through with the demands of the form, the Cox Report sets up an expectation that must be completed outside the text. The vast conspiracy is hinted at but no villain is identified specifically. The Report leaves a gap waiting, wanting to be filled by the identification of a villain, or a scapegoat to represent the vast hidden conspiracy if nothing else is available. Enter Wen-Ho Lee, a pretty hapless villain by any standards until he is reconstructed through government actions and texts and various media reports.

The Cox Report created a need for a scapegoat, and it had to be a scapegoat doing classified research in one of the areas the Committee specifically concluded the Chinese would target. The report concluded that the Chinese, who already had information on miniaturization presumed to be from previous espionage, would most of all want information on computer codes used to simulate explosions. Because they had signed the Nuclear Test Ban Treaty, the Chinese could not conduct tests on their new-and-improved W-88 style warheads (assuming they could produce them, that is...). The so-called "legacy codes," which draw on the data resulting from all of the previous U.S. tests and run simulations of proposed new designs based on that information and what is known of the laws of subatomic physics, were the primary target according to the Cox Report. Lo and behold, enter Wen Ho Lee, a foreign-born researcher working on precisely that project. The plot line is as predictable as a James Bond novel.

ESPIONAGE IN THE CONTEXT OF SCIENCE

The context for Lee's case can be seen as the politics of that time. For those who had vested interests in maintaining the defense budget, and for those unable or unwilling to shift out of the Cold War mentality and its simple black/white dichotomies, there seemed an inclination to replace the fallen USSR with a Chinese Red menace. This trend in U.S. political discourse has all but vanished with the beginning of the war on terrorism, but in 1999 this strong dichotomy

provided an easier way to understand foreign affairs, helped to erase domestic differences, and otherwise served to shift responsibility for anything that goes wrong to "the enemy." These are all symptomatic of the Paranoid Style. The fact that the introduction is by Caspar Weinberger, Reagan's Secretary of Defense, instead of by somebody related to the CIA or FBI, the usual organizations responsible for espionage-related activity, suggests that either the authors themselves or their preferred audience had military implications uppermost in their minds. This is about preparing for war, not the genteel spying games that all nations play.

The fact that the Lee case also occurred in a scientific context carries additional implications. The scientific context provides a variety of alternative rhetorical strategies that are not relevant in other examples of espionage. Secrecy is counter to the norms of most scientific communities, an observation formally made by Robert Merton in 1942 ("Science and Technology in a Democratic Order," Journal of Legal and Political Sociology, v. 115). This widespread norm has been in place since the early 18th century[30] and remains true today. Granted, there are counter-norms available for scientific rhetors to draw upon[31], and there are differences among the various scientific communities regarding this norm. Nevertheless, conventional wisdom suggests that without the free and open exchange of ideas, the idea of progress is impossible, and this is true not only in science but also in all fields of knowledge. As Newton himself reputedly said, "If I am able to see farther than others, it is because I have stood on the shoulders of giants." Or, as Burke notes in his Rhetoric of Motives, "In the past, the great *frankness* of science has been its noblest attribute, as judged from the purely humanistic point of view. But any tendency to place scientific development primarily under the head of 'war potential' must endanger this essential moralistic element in science." (p. 35, emphasis in original)

In 1982, the National Academy of Sciences, Engineering, and Medicine produced a document at Congress's request regarding the harmful effects of secrecy in science. They

conclude, "Controls [over scientific communication] *could* be seen to strengthen national security by preventing the use of American results to advance Soviet military strength. But they can also be seen to *weaken* both military and economic capacities by restricting the mutually beneficial interaction of scientific investigators, inhibiting the flow of research results into civilian and military technology, and lessening the capacity of universities to train advanced researchers. Finally, the imposition of such controls may well erode important educational and cultural values." (p. 3, emphasis in original)

Because the effects of secrecy are considered so damaging, the national laboratories in the U.S., including our two remaining weapons laboratories[32], had been moving towards greater openness in the last fifteen years. Programs for visiting scientists, including those from Russia and China, have proliferated, with an average participation rate of 1500 scientists per year at Los Alamos alone[33]. The Cox Report set back this trend by creating an atmosphere of secrecy and paranoia in scientific circles. For example, the second chapter of the Report, which purports to describe how the presumed espionage might have taken place, mentions essential public events such as scientific conferences and official diplomatic visits. It states, "The China Academy of Engineering Physics has pursued a very close relationship with U.S. national weapons laboratories, sending scientists and senior management to Los Alamos and Lawrence Livermore," (p. 111), "The PRC relies on a variety of methods to acquire military technology, including illegally transferring U.S. military technology from third world countries and applying pressure on U.S. commercial companies to transfer licensable technology illegally in joint ventures, and exploiting dual-use products and services for military advantage in unforeseen ways." (p. 54) The effect was, ironically, after a decade of increasing programs to encourage scientific exchange and thus strengthen international relations, the Cox Report reverted the national labs to a Cold War state of mind, even to the point where Bill Richardson (then head of DOE, formerly Senator R-NM) ended the programs allowing foreign scientists to visit and

collaborate. Shortly afterwards, Richardson repealed the ban, and in publicly defending his decision against the complaints of various Congressmen, he stated, "As a result of congressional hysteria over security, we are in danger of losing the science that we sought to protect. I want to restore the proper balance between security and science." (quoted in Washington Post, p. A11, December 3 1999) The exchange programs were not taking place in secret, they were and are approved and funded by Congress. So the tone of surprise and alarm in the Cox Report regarding the amount of interaction between our national laboratories and Chinese scientists is certainly unwarranted, and seems to be part of a rhetorical strategy of scapegoating.

Scapegoating is, for Burke, a process by which a community designates an individual or group of individuals as laden with the community's sin, and hence responsible for the ills visited upon the community. By casting internal problems onto an "other," the community is able to externalize and then eliminate the guilt by eliminating the scapegoat. Scapegoating is a common response when events have gone awry. Given the severity of the calamity depicted in the Cox Report (regardless of whether or not the events occurred as suggested or whether, even if they did occur, the events merit such treatment), it is hardly surprising that the Report engages in a certain amount of scapegoating. In fact, the surprise is that the Report doesn't do more scapegoating. The national laboratories are criticized for their lax security procedures (Report, p. 121-124), and the industrial weapons manufacturers are criticized more than any other party involved (and the criticism is particularly harsh in that it ties their faults to greed instead of naivete, as was the case with the national labs). For example, on p. 25, the Report states in a bold, 14-point font, "U.S. policies relying on corporate self-policing to prevent technology loss have not worked. Corporate self-policing does not sufficiently account for the risks posed by inherent conflicts of interest, and the lack of priority placed on security in comparison to other corporate objectives." No individuals are blamed, nor are any groups of individuals singled out.

A rhetorical strategy in which such grievous crimes are depicted, however, demands more specific judgements than simple systemic flaws. The Report sets up a need for a scapegoat, even as it fails to provide one within the text. Before the end of the year in which the Report was published, a major spy-scandal appeared in the mass media, conveniently providing that scapegoat.

ENTER WEN-HO LEE

Wen-Ho Lee was in many ways the ideal scapegoat set up by the Cox Report. Because he was born Taiwanese, a simple and straightforward motive was presumed during early stages of the investigation into China's nuclear espionage. Taiwan is officially still part of China, and the assumption that a native Chinese citizen would be inclined to spy for China was a part of the operational assumptions of the CIA, the FBI, and the Justice Department. This operational assumption is in fact the basis for the defense lawyers' strategy of arguing racial profiling. Illogical though this may seem in retrospect (after all, the CIA is certainly aware that many Taiwanese citizens often are quite actively opposed to China), Lee's ethnicity was listed on every single document as a viable reason for suspicion: in the Administrative Inquiry submitted by the CIA to the FBI, in the wiretap requests submitted by the FBI to the Justice Department, and in Justice Department prosecutors' arguments to deny bail. Conventional wisdom within the intelligence organizations held that China's preferred espionage method involves recruiting ethnic Chinese to share classified information with arguments that they would be helping their worthy and badly disadvantaged homeland. This assumption was so widely and unquestioningly believed that it served as one of the primary justifications in each of the ever-widening steps in the Lee investigation, which was code-named "Kindred Spirit." The first step, conducted by Notra Trulock and Dan Bruno, involved the preparation of an Administrative Inquiry, a document compiled by the CIA to persuade the FBI that they should open a casefile and dedicated sufficient resources to conduct a preliminary investigation. This Administrative

Inquiry formed the basis for subsequent actions and arguments, and contains the seeds of what later led to the downfall of the prosecution's case against Wen Ho Lee.

To understand the role of the Administrative Inquiry, it is necessary first to understand the unique structure of the U.S. Intelligence community. There are numerous intelligence-gathering branches of the federal government, and intelligence is collected relating to both foreign and domestic affairs. Almost all of the agencies are fairly new, having been created within the last century, and largely as a product of U.S. experience in World War II. The CIA nominally has responsibility for coordinating all foreign intelligence, including any covert action and any counterintelligence activity. The FBI nominally has no foreign intelligence responsibilities and has sole responsibility for any domestic intelligence. These divisions, while clear in theory, in practice are not readily ascertained and are frequently set aside. The divisions are one of many sources of tension between the CIA and the FBI. Historically, the two primary federal intelligence agencies have been openly antagonistic, ever since their founding. Espionage cases are investigated by the FBI, because espionage involves criminal charges against a U.S. citizen, which can only be brought for prosecution by the FBI in coordination with the Justice Department.[34] The CIA and the FBI often have competing interests in regard to espionage cases. The CIA would like to either "turn" the spy (use him or her to feed false information to the foreign country) or at least end their access and compel assistance with damage assessment, while the FBI necessarily wants a prosecutable case with minimal waste of resources on the investigation. An espionage investigation can be a rather long-term and expensive (in terms of manpower and technical resources) process, because the only way to be certain of a successful prosecution is to catch them in the act of physically handing over to a foreign espionage agent clearly classified documents. The CIA is the agency that is most likely to discover initial grounds for suspicion, but they cannot move towards prosecution except by

providing the FBI with sufficient evidence to persuade them to commit the necessary resources for trailing the suspect, tapping phone calls and other communications, and other measures as necessary. The tension between the two agencies means that the CIA as well as the FBI is often reluctant to undertake the necessary steps. Many times the CIA has simply shuffled a suspected spy to a different assignment[35], one which would provide them fewer opportunities to access useful information or to convey information to their presumed "handler." In cases where prosecution is undertaken, the first step is for the CIA to prepare an Administrative Inquiry which sets forth their reasons for believing the investigation should be made. The FBI in turn must persuade the Justice Department to authorize wire-taps, or to authorize warrants to search the suspect's home or workplace. There is a special procedure for national-security related authorization requests, which enables the Justice Department to hear and decide on such requests in secret, but the criteria for authorizing officially remain the same as for any U.S. citizen suspected of any other crime.

Because Lee at one time worked at Los Alamos National Laboratory (LANL) in X-Division, the officially designated group responsible for improving U.S. nuclear weapons, the opportunity for espionage was available and believable. Even better, the research Lee had been conducting had been analyzing data from previous nuclear explosion tests, an area of research which the Cox Report had singled out as one which the PRC was likely prioritize for espionage. On p. 114, the Report states:

> "The ban on physical testing to which the PRC agreed in 1996 has increased the PRC's interest in high performance computing and access to sophisticated computer codes to simulate the explosion of nuclear weapons. The Select Committee judges that the PRC has likely developed only a very modest complement of codes from inputting its own test data. The PRC would, therefore, be especially interested in acquiring U.S. thermonuclear weapons codes for any new weapons based on elements of stolen U.S. design information."

Conveniently, that is precisely the research Lee was engaged in at Los Alamos, referred to in the mass media most often as "legacy codes."

Enter The Media

The New York Times headline on March 9, 1999 broke an exciting news story. "U.S. Fires Researcher Suspected of Giving A-Bomb Data to China," it declared on the front page. This headline was the first linking a specific individual to an espionage investigation that had been ongoing, sporadically and secretly, for the previous four years. Naming an individual to play the role of the villainous spy raised the case to a much higher media profile. But that higher public profile obscures the fact that in some ways the denouement of the case had already been determined, including the media's role in establishing the character of the newly-named villain: Wen-Ho Lee, 61, a researcher in Los Alamos National Lab's top-secret X-Division. So while the New York Times headline is in some ways a beginning, it is also a conclusion, perhaps a foregone conclusion.

The media coverage of the Wen Ho Lee case has been criticized frequently, and Lee's filed a defamation lawsuit against the NYTimes. The criticism comes from the media as well. The New York Times ran a two-part review article, reasoning "In the aftermath [of the Lee case] the government was roundly criticized for its handling of the case; so was the press, especially the New York Times. In an effort to untangle this convoluted episode, The Times undertook an extensive re-examination of the case, interviewing participants and examining scientific and government documents, many containing secrets never before disclosed" (NY Times, Feb 4 2001, p. 1). The re-examination ran over the course of two days, covering ??? inches of column space. To put this in monetary terms, given that the Times charges ??? for one column inch of advertising, the Times essentially spent ??? to defend itself against the criticisms leveled against it. In the end, the Times' re-examination did not result in retracting anything that they had

previously published, but the effort of re-examining in and of itself serves as a journalistic "mea culpa."

Two primary and closely related problems the media coverage of the Lee case have been highlighted. One problem is the difficulty of finding two or more sources to independently verify a claim before accepting it as a fact, as journalists are supposed to be trained to do. But "independence" of sources is problematic, especially in the world of counter-intelligence. Over-dependence on government sources is a widely recognized problem for journalists[36], and this seems to have been exacerbated by the nature of espionage. Espionage is a secret crime, so there are no eye witnesses to interview, no victims to provide heart-wrenching stories; the only source of information possible is the various branches of government involved. If these government sources are influenced by one another, as they were in the Lee case since the only information anybody had initially about the "Kindred Spirit" investigation all came from the series of 81 briefings organized by Notra Trulock, then a bias in one would bias the entire coverage.

The second problem evident in newspaper coverage of the Lee case is the danger of writing with an overly-prosecutorial bent–that is to say, of assuming guilt rather than innocence, as our Constitution requires[37]. The New York Times in particular, the newspaper which first broke the story, has been accused of a prosecutorial bias. This presumption of guilt can be seen in the word choice for their headlines. For example, out of the 124 headlines in the major national newspapers that appeared during 1999, 31 of these referred to Lee as "Suspected Spy" or "Spy Suspect." Technically, this can probably be defended as an accurate description, so that no newspaper is likely to be found guilty of libel using such language. However, the word "suspected" is stronger than "alleged" or "accused," and the dictionary defines the word as meaning "to believe to be bad, wrong, harmful" or "to think it probable or likely" or "to view with suspicion." (Webster's New World Dictionary, 3rd edition) With only one exception, the last occurrence of the word "suspect" in a headline was on August 17, and with only two

exceptions the headlines including that word appeared in the New York Times and the Washington Post. The Los Angeles Times, with its much higher percentage of Asian Americans in its audience, avoided such assertive language, preferring more neutral phrases such as "Atomic scientist" or focusing on federal involvement. The fact that no such words were used after August, even in the New York Times, is not coincidental. On August 22, 1999 Lee's lawyers first began working on the case, and shortly thereafter media coverage changed dramatically. But even though all charges of espionage were dropped and the plea-bargain was reduced to one count of "mishandling," the New York Times in their two-part expose reflecting on the case continued to refer to Lee's behavior as "suspicious," and criticized the government for bungling the investigation and prosecution rather than acknowledging their own role and the harms caused by this (admittedly quite routine) presumption of guilt in the mass media. "I simply reported the facts, it is not my responsibility what implications others draw from them," said Jeff Gerth, the co-author of the Times' early investigative articles on the Lee case. His editors defend his coverage, saying "we simply report on events, we don't influence them." (Interview, The Nation, June 2001) And never mind that the FBI, during an attempt to intimidate Lee into confessing to espionage, used the article as evidence that the espionage was already known by everybody and therefore failing to confess merely postponed the inevitable.

The "overly-prosecutorial bent" in the New York Times coverage is typical of most journalism. The pattern becomes widespread, and eventually almost normative, because of narrative pressures. A story about a criminal act is assumed to be more exciting for readers and is simpler to construct because the roles are so clear-cut and familiar. In the end, the guilt or innocence of the individuals named , at least in the minds of the wider public, has less to do with the facts of the case as presented in a legal courtroom, and more to do with whether a news-worthy story line can be constructed around the verdict after the initial reportage maximizing the shock of the crime.

In the case of Wen Ho Lee, the story-line was gripping both before and after the legal verdict. The coverage changed quickly once the pro-bono legal team had been arranged.[38] Two changes occurred almost immediately: Headlines referring to Lee as "Chinese Spy" were eliminated. The phrase "Chinese spy" (or close variants) appeared in 26 headlines during 1999, before the defense team was arranged. This phrase was an interestingly ambiguous construction. It can be taken to refer to the accusation that Lee was spying for China, to highlight the difference between this case and the usual expectation that if one spies, one spies for Russia. It can also be taken to refer to Lee's ethnicity, though it is a misleading elision used that way; technically, it can be argued that since Taiwan was and perhaps still is part of China, an individual from the island might be called Chinese, but to collapse the two categories ignores important distinctions that matter tremendously in imputing motive. No newspaper article that I read clarified this ambiguous phrase, though some avoided using it from the beginning. Variants such as "China Steals Nuclear Secrets," or "Nuclear Scientist Sells Secrets to China" avoid the issue altogether while still displaying the same prosecutorial bias. Only two headlines referred explicitly to Lee as Taiwanese, but after September of 1999 the phrase is simply avoided altogether, in favor of references such as "Nuclear Data Downloading Defendant" or simply his name. This change is crucial to the public construction of motives, given that the Taiwanese have no more reason to want the Chinese to have far-reaching nuclear weapons than the U.S. has.

The other difference in media coverage after August 1999 is that information about Lee as an individual began to emerge. The legal team made available interviews and photographs of him and his family, for example. Particularly prominent were the quotes from his daughter Alberta, who had arranged the connection to the California law team. Previously Lee had been a cipher in the coverage of the case, which made sympathy for the so-called spy more difficult. Adding a visual component to the rhetoric of the case was advantageous to Lee's defense. Lee's

interview on "60 Minutes" on May 6, 1999 was his first and only television appearance, but many photographs became available, including heart-string-tugging photos of Lee's 61st birthday party with his family gathered around. Lee's "60 Minutes" interview was the nation's first introduction to the man himself. He appeared diminutive and somewhat frail, calm and articulate, rather "grandfatherly" as one editorial writer described him. He looked neither particularly dangerous nor particularly foreign, though his accent hurt his cause in that regard.

Another interesting aspect of the press coverage of the Lee case is the peculiar emphasis placed on his role as a nuclear scientist at Los Alamos National Laboratory. In sixty-one headlines out of 225 that appeared in 1999 and 2000, "Los Alamos" is used as an adjective to describe either the case or the suspect. In other words, almost one fourth of all articles use the "Los Alamos" descriptor as a short-hand reference to distill the significance of the story. We do not know why, but we can speculate about the effect of the rhetorical work this name is doing.

One answer might be that the work done is incidental. The story first became a major news story when Lee was fired, which would as a side-effect necessitate naming where he was fired from. Later coverage perhaps continued to use "Los Alamos" as a safely neutral adjective to describe the case as a matter of consensus. After all, it was no longer agreeable to refer to it as a "spy case," since there had been no indictment on espionage charges. Describing the case as a "nuclear secrets" or "atomic secrets" case was a marginally more common label, appearing sixty-six times. The appeal of a label such as "nuclear secrets" or "atomic secrets" is easy to understand, given that the goal of a headline is to excite maximum interest in order to attract readers and thus sell papers. The use of words like "nuclear" accomplish this by appealing to widespread fears about the dangers of nuclear weapons. The difficulty would be instead to understand why the label "nuclear secrets case" did not become by far the most common descriptor, and why instead the adjective was used less and less often as the case progressed, while the "Los Alamos" descriptor remained relatively constant over time.

By the middle of 2000, press headlines also had begun to refer to the trial as the "Lee case," avoiding any use of adjectives and assuming that audiences would already be sufficiently familiar to find the name by itself attention-grabbing.

Another approach to answering the question of what rhetorical work "Los Alamos" is doing in these headlines would be to attempt to consider what the newspaper's audience is likely to believe the word signifies.

Understanding the Significance of the "Los Alamos" descriptor

As a physical place, the visual significance of Los Alamos is an odd temporality: a union of the distant past (ruins, mountains) and the foggy futuristic (the haze of research), in both cases with an eye towards eternity. The present becomes lost as ephemeral and neglected, as seen by the generally haphazard and random buildings (Los Alamos has had a perennial housing shortage, and hence housing is cheap and mass produced, but the relatively wealthy owners then modify the properties, creating a disparate architectural melange), the lack of material associations such as shops (especially clothing and cars), and so on. The symbolic value of Los Alamos is best summarized by the title used for the Redmond report on the laboratory system: "Science at its Best, Security at its Worst." The associations with secrecy and the breach of secrecy have been closely tied to the history of Los Alamos since its beginning.

The history of Los Alamos has been written about numerous times previously, perhaps best in Los Alamos: The First Forty Years by the Los Alamos Historical Society. The town is best known for its role in World War II. But its history and setting have other resonances as well, shaped by its roles both as a community and as a national icon.

The first residents of Los Alamos were the Anasazi indians. The Anasazi vanished long before Europeans first came to America, and nobody knows why. It was almost certainly not military conquest, because the caves in which the Anasazi dwelt would have been virtually impregnable by any other people of that time. The Anasazi caves are honeycombed across

numerous cliffs and are still available today. The caves are a great mystery, a secret that we have been unable to break. They resonate with the security issues that surround the symbolic meaning of Los Alamos as the site of nuclear weapons research.

The geography of the area lends itself to secrecy and security. Los Alamos today is built on three contiguous mesa tops. "Mesa" is the Spanish word for table, and the mesas are referred to as such because they rise steeply, with vertical cliffs averaging about 10 stories high, and then end abruptly with a flat top. The majority of the rock in the area is volcanic, a mineral formation called "tuff," which is relatively soft and easily carved to form handholds and crude stairs in the cliffs. The volcanic rock is interspersed in places by firmer rock, and hence natural erosion creates the striking mesa-structures. Surrounding Los Alamos on three sides, the Jemez Mountains rise dramatically, and the remaining side proceeds down steeply 500 feet to the city of Santa Fe some 40 miles south.

General Leslie Groves' criteria for a site for the top-secret Manhattan Project required a location that was far from any oceans (hence inaccessible by the enemies), sparsely populated, and preferably ringed by hills to provide further protection against spies. The mountains surrounding Los Alamos, with the relatively flat space at the center, were ideally suited for it. A single road leading into town could be blasted out of the relatively soft rock of the cliffs, but no other easy access would be possible. (Later a second road was built, leading further up into the mountains, which Los Alamos residents refer to as the "back gate.") Oppenheimer had spent time near Los Alamos in his youth, so he knew of the spot, and Groves and Oppenheimer agreed that it would be the perfect place to build a top-secret town. Hence Los Alamos, New Mexico became the home of the Manhattan Project, the gathering place for researchers attempting to build an atomic bomb. [39] Most of the important names (Einstein, Szilard, Teller, Bohr, etc.) and events will be familiar to anyone with any interest in history of science or American History.

For all of the stringent security measures taken to protect the biggest secret of the American war, and for all that the location was inaccessible to non-participants and completely unknown as a spot of any strategic importance, even so there were spies involved in the history of the Manhattan Project from its very inception, as noted earlier in this chapter. Thus, the history of Los Alamos in the public mindset was intertwined with issues of secrecy and espionage from the very beginning. The lessons that personnel at Los Alamos Laboratory took from these episodes of espionage was precisely the importance of secrecy. This was a hard lesson for most scientists, many of whom lobbied the government to share their research with all of the Allied countries after the war. Numerous articles in scientific publications such as the Bulletin of the Atomic Scientists argued that there never was a big atomic secret: the basic principle of the bomb was already widely known, and the production techniques could be readily discovered–perhaps a better means discovered–by anyone with a serious interest. Whether or not this was true, within ten years after the war, four other countries had developed atomic weapons (Russia, Britain, China, India). And a U.S. journalist with little scientific training was able to put together a complete recipe for the Hydrogen bomb based on openly available sources as early as 1962 (see US vs Progressive), only 10 years after the first test detonation of a Hydrogen bomb.

The population of Los Alamos after the war dropped rapidly from its war-time peak of about 5500, but with Truman's decision to push forward development of the Hydrogen bomb, the population stabilized, and the decision was made that the laboratory would become permanent. Transfer from military control was a slow process, requiring more than fifteen years. The war-time buildings remained predominant architecturally, a ramshackle group of houses and laboratories (the section of town that was considered most "posh" was called "bathtub row," since those were the only houses with private bathtubs–all the others were converted military barracks with only standing showers). As the population grew, more permanent houses began to

be built along the tops of neighboring mesas, and even on the plateau below the edge of the primary mesas, which became the satellite community now called "White Rock." Families began joining the scientists employed at the lab.

Until 1957, Los Alamos remained a gated community, with the only two roads in or out guarded and manned 24 hours a day. No personnel were allowed to enter or exit without a security pass and proof of their identity and appropriate business and clearance. No private industry, shops, or service industries were permitted in Los Alamos itself, though in nearby White Rock a basic grocery store and a few restaurants were opened. In Los Alamos, a school district and the necessary support functions had to be established, but until 1975 the school district was run by the AEC (later DOE), operated on the same basis as the schools at military bases in foreign countries. Banks and other necessary service industries were also operated by the government through a contracting agency. Local government was in the hands of civilian personnel working at Los Alamos–basically, scientists with an interest or aptitude for organizing the very minimal county government. Establishing local government proved one of the largest hurdles. The state government was reluctant to recognize the diminutive county as having equal representation, and the AEC continued to exercise autocratic control over all the decisions which mattered, since government still owned all of the property until 1965 (houses were rented, and maintenance was performed by a government contractor called Zia Company). When Leslie Groves, the Army general responsible for the Manhattan Project, had chosen the Los Alamos site, the land purchased was made into a separate county, and after the war it was necessary to develop a Los Alamos county police force and ambulance service. The federal government subsidized all of these functions in the county, only gradually reducing its role over the course of the 50's and 60's. During the 1970s the lab began branching out, extending its mission to include research other than strictly nuclear or even strictly military-related. Los Alamos National Laboratory began to include research on alternative energy sources (solar and geothermal in

particular), environmental matters, biological and medical matters, chemistry, and above all computers.

The lessons regarding secrecy had perhaps been learned too well by the management of Los Alamos National Laboratory. During the 80's, public controversies embroiled the lab, and the management's response to those controversies reveals how closely they held to their secrets. In all cases, the official laboratory reaction to the public outcry was the same: these are national security matters, and as such we cannot and will not discuss these matters with the public. Yet this response has not stopped public controversies from erupting.

Reagan's Star Wars (Strategic Defense Initiative) program of the 1980s proposed to build an anti-nuclear weapon defense system in outer space, so that the U.S. could not be threatened by nuclear warheads. The primary proposed version of this was to set in orbit a satellite that could shoot out laser beams that would target the warheads in mid-flight and render them harmless, either detonating in the air or knocking them off-course into the oceans. (Later presidents, when they revive the notion of a missile defense shield, have relied instead on ground-based missiles which would again target the warheads in mid-flight and destroy them.) The opposition to Star Wars was huge. It would violate an earlier international treaty that had agreed not to use outer space for weapons of war, it would be hugely expensive, and as scientists were quick to point out, it was unlikely to ever work effectively. Protesters conducted demonstrations in Santa Fe, and attempted to confront laboratory management, but were stopped by the Los Alamos security force (laboratory security is handled by a contractor working directly for the Department of Energy, and thus is managed separately from the scientific personnel; this separation was one of the primary structural criticisms raised in the Redmond Report in 2001).

A similar pattern developed in the public controversy over the Waste Isolation Pilot Project (usually referred to as WIPP), which involved storing nuclear waste in barrels underneath the same desert where the first atomic bomb was tested (the Trinity site, a passage of land called

by the Spanish Conquistadors Jornado del Muertos, or Journey of Death, because the desert proved unpassable for the explorers). The storage proposal necessitated shipping the waste from Los Alamos through Santa Fe and thence to the desert (remember that access in and out of Los Alamos is still extremely limited, there are no other roads or easy ways of making other roads). The Santa Fe community was horrified by the idea. Rather than explain to their nearest neighbors what safety precautions were being taken or otherwise communicate about the issue, the laboratory response was that this was all classified information (remember that the criteria established for classification require that it cause "material and irreparable harm to the national interest" should an enemy nation learn of it), and the Santa Fe citizens did not have clearances and so could not be told anything about it. Tensions between residents of the two communities became sufficiently strained that vehicles with Los Alamos license plates were occasionally vandalized if parked in Santa Fe. WIPP experienced other setbacks and was delayed until 1992, at which time laboratory management was working towards a new openness under the Clinton regime.

The end of the Cold War encouraged openness at the lab both domestically and regarding foreigners. Even during the height of the war, guarded exchange programs between Russian and U.S. nuclear physicists were allowed, both nations recognizing the potential benefits to be gained from the exchanges. And visitors from allied countries were often brought to the lab, though no country had full access to the highly classified materials handled by X-Division. After the Cold War, exchange programs expanded tremendously. Community outreach programs were also begun, with the organization's management chart shifted to give higher priority to these programs. Additionally, the programs for students were expanded tremendously during the 90s, bringing in record numbers of undergraduate and graduate students for anywhere between one month to three years. But the increased openness was not universally favored: the security force scrambled to find sufficient employees to keep up with the new growth, often failing because of

budget and time constraints. The Department of Defense provides partial funding for certain projects at the lab, and DOE and DOD often disagreed regarding security measures. The issue was also politicized, with Republicans favoring greater emphasis on security through secrecy while Democrats took up the scientists' argument from the 1950s that security is better achieved through improved science, which can only be accomplished when diverse scientific viewpoints have the opportunity to collide. In such an atmosphere, it was perhaps inevitable that the contentions over security measures would result in heightened scrutiny, and perhaps inevitably a spy scandal.

The Russians have not been able to duplicate their war-time penetration of Los Alamos National Lab. The initial glut of atomic spies was made possible by two factors: our war-time alliance with Russia, and the relative increase of the American Left during the 1920s and 1930s. The war-time alliance meant that many Russians, including military personnel, were in the United States for legitimate reasons, arranging the transfer of arms to help defeat the Nazis and arranging exchange of food and medical supplies. The Russians were our allies, and as such many members of the Allied nations did not see them as a threat, and requests for information were not regarded as suspicious. Additionally, the 1920s and 1930s had seen the rise (to threatening proportions in the eyes of the government) of the International Socialist Workers Party, and affiliated workers sympathetic to the Communist philosophy. This trend was thwarted by the harsh use of the 1917 Espionage and Sedition Act to cripple the party's leadership, and later by McCarthy and the House Un-American Activities Committee (HUAC), which denied anyone affiliated with organizations sympathetic to Communism employment, and gave the FBI free reign to monitor and blackmail anyone involved in such activities. Throughout the 1950s, scientists as well as others were hauled in for HUAC hearings, and leadership at LANL was decimated by the investigations. Oppenheimer is the most famous such case (he lost his security clearance and hence his job), but additionally Oppenheimer's Deputy Director, Edward Condon,

was denied a security clearance, as were an estimated 400,000 other scientists (David Caute, The Great Fear, as quoted by Jessica Wang in "Science, Security, & the Cold War").

In the fifty years since the war, the big spy scandals have involved the CIA, the FBI, and the Navy, but not Los Alamos. There have been smaller, less publicized prosecutions for espionage or related activities among scientists involved in classified research. It also is likely that many cases of espionage or suspected espionage never go to trial and are never publicized. Security inquiries are routine at any workplace that handles classified materials, since clearances need to be renewed regularly and spot-check investigations are performed as a matter of course (one of the other criticisms in the Redmond Report is that Los Alamos security, because of the increase in personnel, had reduced both the frequency and the randomness of these checks, but this is not to say that they had completely stopped). It is impossible to guess how many employees were quietly transferred from a highly sensitive position to a position with a different research group or a different project within the same group. And certainly it is a matter of routine that other countries attempt to penetrate security at Los Alamos and other labs via questioning scientists visiting their country or at conferences, via searches of the literature, and via questioning and carefully preparing their own scientists who work abroad at various points. This routine security work is a very different matter from an actual espionage prosecution, in that no extensive investigations are involved, no opportunity for defense is involved, and no publicity is involved.

Two espionage trials in particular are worth noting. In 1985, a Los Alamos scientist named Sam Morison was convicted of espionage. He had given a picture of a Russian aircraft carrier to Jane's, the British publication internationally known as the best compendium of information on weapon systems (airplanes, naval vessels, and tanks in particular). The issue was that the picture had been taken by United States spy satellites. Arguably, the picture revealed the satellite's capacity, the level of detail of which it was capable, in a way that was detrimental to

national security. The counterargument is that other pictures from the spy satellites were already publicly available[40], and that moreover anyone interested can calculate the power of our spy satellites as well as their schedules (this is one of the ways Pakistan managed to avoid detection of their atomic bomb development, for example, and the calculations based on payload have been published by historians engaged in research in this area). Morison was convicted and sentenced to a large fine but no jail time.

The other espionage-related case that has come to public light involving the national labs is not related to Los Alamos, but rather its sister-lab in California, Lawrence Livermore National Laboratory. Peter Lee was accused and pleaded guilty to selling information to the Chinese regarding computer processor research. This case was reported extensively in the media only ten years after the case was closed (Peter Lee was suspended from his work on classified subjects but continued to be employed by LLNL), when another Lee became famous. Wen Ho Lee, it turns out, had contacted Peter Lee while Peter Lee was being investigated. Wen Ho asked if Peter needed any help, an offer presumably provoked by sympathy for a fellow Taiwanese-native and fellow-scientist, but perhaps motivated instead by reasons of shared guilt, or so it seemed at the time.

So it seems likely that the use of "Los Alamos" as the descriptor for the Lee case is serving to signify both espionage and nuclear weapons. The phrase is useful because it performs all of the rhetorical work done by the both of the common phrases "nuclear secrets" and "spy case," via connotative reference chains. Like an enthymeme, the use of the name involves the audience directly by asking them to supply the missing premises, or in this case the unstated presumptions. But as with any persuasive appeal designed to be effective using the paranoid style, the term signifies different things on different levels. For an audience interested in espionage to begin with and therefore "in the know," the term is more likely to evoke security breaches and dangerous international competition. For an audience less accustomed to the

search for hidden significance, the descriptor "Los Alamos" stands as a relatively innocent, "factual" reminder of previously-stated background information regarding the trial.

The Lee case goes to trial

The judge's apology at the end of the Lee trial was particularly striking because it represented a radical departure from the his stance at the start of the trial. The judge only reluctantly accepted Lee's plea-bargain. Lee plea-bargained, agreeing to plead guilty to one count of mishandling information after the other 68 were dropped, and was sentenced to time already served. The judge is the same one who, ten months earlier, had sentenced Lee to prison without bail and in solitary confinement. The prosecution had argued that Lee was so dangerous a threat to national security that he could not be released under any form of supervision, and that even when his family visited him in jail they could not be allowed to speak Chinese (the usual language used in the Lee household). But in the end the prosecution's case could not support a single charge of espionage, in spite of the dire presentation made to persuade the judge to hold Lee without bail. Let us now turn to consider more carefully the prosecution's case.

The investigation and later prosecution rested on the presumption that China had stolen nuclear secrets. In other words, it began not with motive nor with evidence of a mechanism of communication, but only with the conviction that somehow communication must have occurred. What convinced the investigators that communication had occurred? The Department of Energy collects data monitoring suspected nuclear weapon tests, including seismic and atmospheric monitoring. A 1992 report suggested that the Chinese had exploded a nuclear weapon, and that the data collected suggested that it might be a smaller warhead design than any that we had known the Chinese to possess previously. The second bit of evidence was a Chinese "walk-in," a Chinese agent who sought out the CIA and left a folder of nuclear weapon-related information. The documents included a diagram similar to the W88 warhead developed in the U.S., and also included documents relating to the W56, the W62, the W76, the W78, the W87. In 1995, when

the walk-in documents were first delivered, the translating process began first with the documents related to the W88, and until late 1999 was the only portion familiar to the FBI or the prosecution team. The CIA had already determined that the "walk-in" was a plant from the Chinese intelligence agency, that the documents were turned over with the approval of the intelligence agency which for some reason wanted us to have the W-88 document and others. Such sharing of information is not unique in the practice of Chinese intelligence. The Chinese concept of *guanxi* led high-level officials in the Chinese nuclear program to invite high-level U.S. scientists to view almost every aspect of their program beginning from 1979 to 1985, with the expectation that the U.S. would return the favor.

What are the chances that the Chinese could independently develop a warhead design similar to the W-88? This is the central question that a committee of scientists debated, eventually disbanding because no agreement could be reached. SSK theorists and practitioners today often highlight the important difference that culture makes regarding what research results, and hence what scientific "knowledge," will be produced. If we accept that cultural differences lead to different "scientific knowledge," then indeed we should expect that China could not have independently arrived at a design similar to the W-88 on their own, and so they had to have gotten the information from us, either legally or illegally. Alternately, we could conclude that the Chinese are not so culturally distinct from us, but this seems unlikely unless we argue that science has already become so internationalized as to be constant across the East-West culture divide. If we accept that science has become sufficiently internationalized across the East-West culture divide, then we could argue that similarity of bomb design is NOT proof of communication, because it could have been independently derived. This is the argument the Chinese officials who have spoken regarding the case asserted, in documents such as the rebuttal to the Cox Report prepared by Hu Side and titled "Facts Speak Louder than Words and Lies will Collapse by Themselves." What, after all, are the parameters within which such a weapon could

be designed? How much variation can there be without preventing the thing from working? It's possible that this provides an argument supporting a rather unpopular idea: that regardless of the researcher's culture or beginning assumptions, physical constraints lead to very specific, particular answers.

Even if we accept that similarity of bomb design necessarily proves that communication occurred, which the walk-in documents do suggest, still this is not proof of espionage. The possibility exists that the information could have been gained legally, and it is also possible that the communication was not with U.S. sources. It is generally well known that China's preferred intelligence technique is to mine open sources primarily, collecting information from numerous, disparate individuals and documents rather than relying on one well-placed spy. The FBI never combed through the open sources to determine the extent to which information leading to warhead miniaturization is available, but there is significant precedent. In 1962 a journalist was tried for having put together information from open sources that enabled him to publish the entire design of our then-most-current warhead (US vs Progressive.). The journalist won the case in that he proved he relied only on open sources, and was thus not guilty of espionage, but was nevertheless prevented from publishing the article. Similarly, the Chinese could have relied on non-classified sources, which are numerous. One error contained within the walk-in documents suggests that this is likely at least for the W62 information, because a characteristic[41] error in the information published in Jane's is reproduced in the Chinese documents. Alternately, the Chinese could have gotten information on warhead miniaturization from the Russians, who had mastered this technology decades earlier, and many of whom are unemployed and doubtless happy to sell their expertise. Therefore, the prosecution's leap to the conclusion that illegal communication (i.e., espionage) occurred is faulty reasoning. But given this conclusion, the decision to prosecute Wen Ho Lee still requires much more evidence.

The leap for which the FBI has most often been criticized was their presumption that if espionage occurred, it had to have been from Los Alamos National Lab. Those who know how science works, and the strong interrelatedness of researchers, should know that knowledge is hardly possible to be isolated in this manner. The walk-in document most central to the Lee case was later concluded to be from "interface documents," information distributed to the defense-contract companies responsible for manufacturing the reentry vehicle and widely available within DOD, DOE, and contractors' offices such as Lockheed Martin. The realization about the numerous other missile data included in the documents also suggests a source outside of Los Alamos, since the majority of the previous missile designs had been developed at Lawrence Livermore. The translation and re-investigation of the full range of the Chinese walk-in documents suggests an array of possible sources in the thousands. This was acknowledged by the FBI in early 2000, when they broadened the search, and admitted that with these new parameters the case would be practically insolvable.

Considering the case made by the defense also highlights the equivocality of information related to espionage. The way in which the audience reads the text can vary the meaning of the "facts" of the case, and can alter the significance of the outcome. For example, consider the explanation given by Lee as to why he made copies of the entire library of classified codes; he has said (in numerous sources) that he was merely making a back-up copy, so that if the computers crashed again at work the codes would be still available. For an audience that relies heavily on PC's, and is familiar with the difficulty that can be caused by the all-too-frequent computer crashes that many of us experience, the argument sounds plausible, even probable. For an audience used to reading in search of hidden clues and suspicious activity that might reveal the always-present traitor within, the argument that Lee was taking responsibility for "protecting" the work of dozens of scientists "for their own good" is an invitation for extended, cynical questioning. For an audience familiar with the security systems in place safeguarding

the mainframes (bear in mind that these are not like the desktop PC's; these are massive, powerful machines staffed by a team responsible not only for their maintenance, but also more often than not the very individuals who built and programmed from the beginning, and for whom this is their life's work) at a national lab, the story also lacks the material coherence that Walter Fisher speaks of as essential to the effectiveness of a narrative.

Post-trial Analysis

The varied ways in which the specific details of the case can be interpreted, and the ways in which contextualizing information alters the stories that can be created from those details, makes particularly crucial for public understanding the compilation of the details into coherent stories. The story form this takes on will most often be biographical. Other types of stories would be possible; for example, a structural analysis (what went wrong with our intelligence system here?) or a different type of history (a history of Chinese intelligence efforts in the U.S.). But as of yet, nobody has attempted to write such a book, because the biographical approach is so normative in cases of espionage. And biographies have very particular effects, particular rhetorical strategies common to them, and require a set of background presumptions. Biographies of nuclear spies, as a popular sub-category within the genre, have their own set of rhetorical constraints. Bryan Taylor explored these issues in reference to a recent biography of Klaus Fuchs, but the arguments he made in the February 2002 issue of QJS, but the arguments are much easier to see in the case of Wen Ho Lee.

> "Biographical texts are particularly useful for examining the organizational cultures and cultural politics surrounding nuclear weapons development. As narratives of personal experience, biographies foreground the institutional micro-practices through which nuclear professionals are constructed and maintained as subjects. ... Biographies of nuclear spies, however, face distinctive challenges and create distinctive opportunities for nuclear culture." –p. 34

"As a Western cultural discourse, biography has traditionally been used to depict the presumably unique identities of individual subjects. Although biographers may negotiate different relationships to this tradition, most operate as 'artists under oath,' sworn to the ideal of transparency in faithfully 'capturing' the subject's essence. At the same time, of course, biographical accounts are assembled from documentary evidence–interviews, newspaper articles, photographs, memoirs, other biographies–that speak in various ways to the subject's behavior and experience in particular institutions. ... Critical focus has shifted to the historical and cultural conditions under which biographical discourse about the subject is produced and consumed."

"Biographies of Los Alamos spies invite this approach. Spies are subjects who compel urgent questions about identity (e.g., as 'loyal' vs. 'disloyal'). During the Cold War, this urgency was exacerbated by virulent anti-communism that sought to purge the U.S. body politic of the contamination of Leftist subversives. Since 1945, massive and highly subjective archives have been produced by agents of the national security state seeking to monitor, detect, quarantine, 'turn,' prosecute, convict, sentence, and execute suspected spies. These records in turn have been resources for dramatic courtroom performances that establish the guilt or innocence of spies, and contribute to their evolving intertextuality. Over time, realist rhetoric surrounding these events (e.g., in news media coverage) has merged with discourses of popular culture that re-articulate the personae of 'real' spies (e.g., as characters in historical fictions), construct fictional characters (such as James Bond), and generally mediate relationships between popular audiences and the evolving national security apparatus. Los Alamos is a frequent site for this blending of fact and fiction."–p. 34

"Biographers of Los Alamos spies, then, must construct their subjects out of vast, buzzing archives. The problem is not a lack of evidence, but a surplus."

"There is a final reason that biographies of Los Alamos spies invite postmodern critique, which stems from the cultural presumption that Los Alamos spies reveal nuclear secrets that threaten U.S. national security. As a result, biographies of these subjects simultaneously are concerned with mysteries surrounding their identities and the technological complexity of nuclear weapons (e.g., in judging the severity of a spy's disloyalty by distinguishing between 'valuable' and 'worthless' secrets passed to the Russian enemy). As practical matters, these mysteries are potently related. Secrecy is perhaps the defining characteristic of nuclear-organizational cultures. Manifest in practices such as background investigations, compartmentalization of tasks, and the encryption of

knowledge in arcane and euphemistic codes, secrecy is both 'the anvil on which the identity of new weapons scientists is forged' and the phenomenological sediment of their senior colleagues. Because these secrets historically have established a quasi-mystical, elite sphere protected from democratic oversight, their revelation in biography potentially affects public perception of the legitimacy of nuclear weapons institutions." –p. 35

" ... These examples join a cascade of others involving the literary underpinnings of nuclear-scientific knowledge, the inability of stolen materials to document tacit designer knowledge required to realize the value of their explicit content, and the increasingly widespread availability of basic scientific theory and design knowledge about nuclear weapons.

Collectively, these contingencies undermine assumptions about persons, technologies, nation-states, discourse, and knowledge that underpin attributions concerning the theft of nuclear secrets. In the realm of nuclear espionage, they ensure that competing discourses of science, national security, and individualism will saturate biographies, and shape their claims.

The consequence of these contingencies is that biographers of Los Alamos spies bear a reflexive relationship to their subjects because both seek truths that can only emerge as equivocal fragments. Both biographers and spies are challenged to deliver the goods and resolve contradictions that often result from the arbitrary imposition of coherence on complex systems of discourse."–p. 36

The biographies of Wen Ho Lee are openly contested, making Taylor's arguments much easier to see. The two biographies that have been published related to the Wen Ho Lee case provide an opportunity to more clearly see the rhetorical construction of competing claims. The two books are the auto-biographical My Country vs. Me, by Wen Ho Lee and Helen Zia, and A Convenient Spy: Wen Ho Lee and the Politics of Nuclear Espionage by Dan Stober and Ian Hoffman.

The two books are competing in several senses of the word. Obviously, each is competing to get the largest market share. The publishing houses responsible for each book (Hyperion and Simon & Schuster, respectively) manipulate the texts to best strategic advantage in terms of the timing for the release of the respective biographies (both in early 2002, but the

autobiographical My Country vs. Me had the advantage of a slightly earlier release date, to better take advantage of the lingering publicity from the case), and in terms of the title selection and front cover images. The front cover images provide an interesting contrast. The autobiography has pale, bright colors (the blue of the New Mexico sky, the white hair of Lee himself, etc.), while the biography has primarily dark, reddish-toned colors, consistent with the common palette for the fictional espionage genre (a glance at the bookstore shelves will verify for you that this trend is non-coincidental–spy novels almost always takes place at night or in the rain). The authors are also competing in terms of establishing their credibility as an authoritative source regarding the topic. And the books are competing as well in terms of what they attempt to leave the audience believing about the fundamental questions involved in the case itself.

Lee's book, for example, is an attempt to shift from the stasis of quality (is he guilty, or is he not guilty), to the stasis of definition (what is this case about?). Lee wants to redefine the fundamental issue involved in the case not as an espionage trial, but as a trial about race relations. With this goal in mind, his book includes large sections addressing evidence of racial bias of all sorts. One chapter deals extensively with the history of prejudice against Chinese Americans, from the brutality of railroad workers to the trials faced in California by Asian Americans and to other instances of racial bias today (such as the arguments of Chinese-American scientists in numerous other organizations that the Lee case brought into the open discriminatory practices, and hence motivated them to realize that the case against Lee was a concern for all of them, and they had to get involved). Another chapter deals extensively with discrimination within the legal system, not just against Asian-Americans but also dealing with the racial profiling of African-Americans in terms of harassment by police and consistent trends towards harsher sentences. Lee does not, however, address the question of discrimination within the context of intelligence and counter-intelligence work. He takes for granted that the audience

will supply the missing premise in his syllogism: discrimination occurred, and discrimination is necessarily always bad, therefore the entire case is bad. But what of an audience that questions that basic presumption? After all, there are only two publicly-known cases of Chinese espionage against the U.S., and in both of those cases the guilty spy was, in fact, ethnic Chinese. Peter Lee, mentioned earlier was one such case. The only other publicly-known case was Larry Wu-Tai Chin, an employee of the State Department who kept the Chinese informed about the negotiating strategy (and the sincerity of those negotiations) of Kissinger and Nixon's administration. Chin committed suicide when he was arrested, leaving behind a note proclaiming his innocence and love for both countries. The knowledge broadly available within the intelligence community is likely not much greater, given the highly-compartmentalized and secretive nature of each investigation. Some within the counter-intelligence community (for example, Bob Vrooman) have pointed out that from what we know based on scientists who report being approached and questioned by the Chinese, the Chinese seem to approach and try to recruit everybody equally, regardless of ethnicity or anything else. We see here again that the validity of the argument itself cannot be judged by itself, but will always crucially depend on the reading of the audience.

Stober and Hoffman's novel fits much more squarely within the constraints of the espionage genre. One example of this is that the focus of the action shifts, from pursued (Lee) to pursuer and back again, building suspense by contrasting the parallel growth of knowledge for each side. The question of discrimination is dealt with only as it becomes a strategic resource for the defense, and as public awareness of the question grows. Because the novel is clearly within the espionage genre, two chapters are devoted to some of the history of Sino-U.S. scientific relations, and to general information about the nuclear weapons and the labs themselves. The wealth of information included in Stober and Hoffman's book about the details of the W88 particularly, and nuclear weapons generally, do little to increase the audience's understanding of

the case itself, but do much to establish the credibility of the authors as knowledgeable and authoritative sources.

Credibility is one of the key arenas of competition between the two books, and the differences in their strategies for establishing ethos are prominent throughout the books. Lee has the advantage of having his credibility in some ways established prior to the beginning of the book; the audience knows who he is, the audience knows that his knowledge of the case comes from his central role within it, and the audience also knows that his knowledge of nuclear weapons and related technical matters is warranted by his physics PhD and his employment at the lab. Because those aspects of his ethos are not contested, Lee spends absolutely none of his time talking about the weapons themselves, though he calls them the "heart of the case." His only comments about the weapons themselves, in fact, comes on page 64 when he says "I even made a list of some specific questions for him [Ken Schiffer, counterintelligence chief at LANL]: What is the W88? What did Carol Covert mean when she asked me if I ever 'worked' on the W-88?" Instead he dedicates entire chapters to discussing his background, his childhood in Taiwan, his family connections, and his arrival in the United States. Strategically this makes sense, because the aspect of his ethos which is most in need of development is an understanding of his motives, of his loyalty and the reasons therefore. His burden is that he must establish for himself the type of character that we would believe would be prone to downloading all of the computer codes just to keep them safe. He must persuade the audience that his loyalty to his family, which he emphasizes strongly throughout, would lead to a loyalty to the United States and not to Taiwan. Lee bolsters this attempt by writing in first-person, and emphasizing that first-person viewpoint by beginning the majority of sentences with "I," by relating his emotional reaction to each event immediately after introducing the event, and by including intimate details of his family-life that are more self-disclosive than is common in any novel within the espionage genre.

Stober and Hoffman are both journalists, working for the San Jose Mercury-News and the Albuquerque Journal respectively. Their ethos as citizens, of course, is never questioned. Their burden is to prove instead a mastery of the complex questions involved in the case. To do this, they cite documentary sources and interviews extensively. Not a single page in the book is completely free from source-citation. Exact quotes are used rather than paraphrases in almost every instance. The notes included for each chapter list the breadth and variety of the sources drawn from, which for each chapter take up roughly half a page (not in bibliographic form, but merely in summary form). Additionally, the authors include a wealth of technical detail about the codes, the weapons, the specific dates and times of events, and other information that Lee largely ignores. Lee by contrast is forbidden to name the commercially-available code that arguably provides more power for the same calculations compared to the code he works on, while Stober and Hoffman are free to name the code and discuss the relative merits of each. Lee is legally constrained, and in order to establish the ethos he desires must avoid anything which might seem to reveal information that might be of use to the Chinese, even when that information is clearly available through other sources.

One of the other differences between the two books is the impression they leave the reader with regarding the outcome of the case. Lee's books draws the conclusion that justice was served, and that the primary lessons to be learned are about the importance of every individual actively voting and safeguarding their civil rights. These are the explicit lessons Lee draws. Implicitly, the primary goal is to demonstrate Lee's innocence, and with that in mind the last three pages actually address for a second time the questions which were most damaging to his case, where his explanations are weakest. Stober and Hoffman end their book with a skeptical ending, and the primary lessons to be learned are the importance of better intelligence methods for the future. The book ends with a series of viewpoints from within the intelligence community, regarding the still-ongoing investigation based on the walk-in documents and

regarding alternate explanations (and question) for Lee's downloading activities. The most telling quote is from former Justice Department chief of Internal Security John Martin, "If a hostile intelligence service wanted to launch a covert operation against the United States, it could not have been more successful in discrediting the criminal justice system, exploiting suspicions of racial profiling, demoralizing the career services of the Energy and Justice departments and the FBI, and diverting investigative attention from other suspects." Another layer of possible meaning is added to the available facts, the strategy of the Paranoid Style is still effective.

The strategies the biographies use to draw these diverse conclusions differ along three primary lines: the ways in which they contextualize the case, their assessment of the damage theft of the codes would have done, and their assignment of responsibility for the case.

Stober and Hoffman make efforts to contextualize the case in relation to the history of Chinese intelligence regarding nuclear weapons. The history includes the role of scientists such as Harold Agnew who began the early exchange programs, and the favor with which the CIA viewed these programs. Stober and Hoffman begin the story itself in 1995, when the Kindred Spirit investigation first began. By contrast, Lee begins the story with his parents' move to Taiwan, and includes small bits of the history of the Communist revolution in China and the impact on Taiwan. When he relates events regarding the case, he contextualizes them somewhat in relation to political events such as elections, but for the most part assumes that the audience already has extensive knowledge of the context surrounding the case, such as the Democratic fund-raising scandal and the increasing tension with China. This assumption seems at odds with the lesson he explicitly draws from his own experiences; that is, if he is urging us to view his case as a reason to become aware of an involved in politics, then it is problematic to assume that the audience will already be familiar with the current events occurring at the time of the case. The assumption regarding context also indicates something of Lee's goal regarding the book. He wants to tell the story as a continuation of his legal case, to achieve vindication in the public

opinion. He is not interested in future audiences, or audiences outside of the United States. The text is driven, in terms of what gets included and in terms of what gets excluded, by a defensive approach continually attempting to deflect accusation, but therefore always assuming that accusation is imminent.

One of the most interesting comparisons between the two books is their assessment of the codes themselves, that Lee was accused of selling to China. Central to any espionage case is the question of harms: what damage was done by the communication in question? Establishing the severity of the loss is crucial for establishing the degree of criminality of the accused spy in the legal system. And the public interest and emotional involvement in espionage comes from the depiction of treason. If the harms done to the public interest are not significant, then the case may involve sales of classified information, but without the requisite demonstration of harms, the case won't weigh on the public judgment the way a case of espionage as treason does. We need to believe that some vital interest that impacts us has been imperiled. Usually, in a case of nuclear espionage, this is relatively simple to establish, because the fear of nuclear weapons is so great. The initial press coverage of the case focused on feeding this fear, with public officials making explicit comparisons between the damage done by Lee and the Rosenbergs. Hence Lee is linked to the start of the Cold War, implicitly raising the spectre of a second long cold war, this time with China. By the end of the case, when the biographies were written, numerous problems with this damage assessment had been highlighted. Both books are in complete agreement that the harm done by the loss of the codes was negligible. But the reasons why the damage is insignificant differ. Lee focuses on the fact that commercially-available (and unnamed, again invoking the power that silence as a rhetorical strategy can provide) computer codes are capable of doing a better job. He notes the age and unwieldiness of the codes, and the fact that entire sections are work-arounds because the original had produced incorrect results

even though nobody understood why. The overall conclusion is that the limitations on the codes are so severe that any country would be foolish to attempt to use them, let alone steal them. Stober and Hoffman comment on the availability of the commercial codes, but are much more keenly interested in the gap between the codes and the materiality of nuclear weapons. Drawing heavily on the testimony of prosecution-turned-defense witness Richter, Stober and Hoffman discuss at length what Michael Polanyi had referred to as the tacit knowledge required to build a nuclear weapon even with all the theoretical knowledge that is available. Additionally, they discuss the ways in which supplies of Plutonium and Uranium are controlled, and the expenses of weapon development. Arguably, these are greater barriers than mere availability of the codes could overcome.

The assignment of responsibility is an important part of a narrative. As noted previously, the expectation that a villain will be provided in a spy novel is as strong or stronger than the expectation of a hero/protagonist. Both biographies suggest names for who the principal wrongdoer was, but both differ as to where that blame gets assigned. Lee blamed the Justice Department, particularly Reno and by extension Clinton. The Democratic party was more responsible for his troubles than the Republicans, as constructed in My Country vs. Me. Stober and Hoffman attribute responsibility primarily to the Republican party, as the party responsible for the Cox Report and many of the most damning quotes. The Democratic politicians involved were treated almost as victims, forced to defend themselves by acting before having time to prepare.

Even at the individual level, the placement of blame differs. Lee saw Trulock as having primary responsibility for the investigation and the problems with it, a view that is more sympathetic with general public opinion because Trulock used the case to gain heightened media visibility for himself. Stober and Hoffman assigned primary responsibility for the problems with the case to Dan Bruno, Trulock's deputy and the author of the original Administrative Inquiry,

with all its attendant flaws. Regarding the legal trial as well, assessment of responsibility differed. Stober and Hoffman gave most of the credit for the legal defense to Cline, in particular for his mastery of the Atomic Energy Act and the details of the nuclear weapons program that enabled a successful CIDA argument (i.e., the arguments that gave the defense the right to draw upon a large array of classified information in an open courtroom, a defense strategy that forces the government to weight the harms done to national security by their own prosecution). Lee gave Holscher most of the credit for the legal defense, and gave himself all the credit for teaching Cline the science that enabled the CIDA defense. Stober and Hoffman give credit for the prosecution's case in its early (and more successful) stages to Richter, Stamboulidis, and to Gorence. Lee gives blame mostly to Kelly for the prosecution's case, taking a somewhat facile approach suggesting that because Kelly was interested in running for office he turned Lee into a high-profile case in order to give himself publicity. The biographies also differ regarding whom to assign responsibility for the public-relations defense of Lee. Lee gives all of the credit to his daughter Alberta, and uses the opportunity to further develop his ethos as a proud and loving father. Stober and Hoffman agree that she was an effective spokeswoman, but give credit for the organizing of the nationwide defense movement and the collection of financial contributions to Cecilia Chang.

The biographies written by Lee and Zia and by Stober and Hoffman were published shortly after the conclusion of the court case, and within a few months of each other. The voice most conspicuously absent in these histories of the case is that of Notra Trulock, who was a pivotal rhetor during the early stages of the case. Trulock's account of the case was published fully two years after the other two books, after most of the public interest had faded. The book was delayed by the review processes of DOE and the CIA. Because Trulock held a security clearance at an intelligence agency, he had signed an agreement that any publications could be vetted for classified material, and in this case two agencies had claims to control some of the

information involved. The result is that Trulock's book actually contains less detailed information than Stober and Hoffman's book on key issues related to what information was purported to be stolen, and what evidence was collected to support this assertion. Trulock provides no new insights into the material issues, but provides a wealth of insight into the personalities and maneuverings that led up to the unsuccessful attempt at prosecution. Trulock places most of the blame on two factors: the arrogance of LANL scientists who balked at every counterintelligence measure, and the laziness of the FBI agents who saw more opportunity for political gain by fighting drug-related crime during the Clinton administration. The arrogance of the LANL scientists is a familiar theme, as it was prominent in Redmond's scathing review of DOE security measures, and had earlier been a theme in the hearings against Oppenheimer and other early nuclear scientists (Wang, 1992). Trulock does not seem to believe that Lee gave the secrets of \nuclear warhead miniaturization to the Chinese, and in fact maintains that Lee was not the leading candidate on the list of suspects at the time when his office was the lead agency in the investigation. Trulock argues that Lee was the FBI's leading candidate precisely because of their experiences interacting with him and his wife in their capacity as informants for the FBI. Trulock highlights the suspicious behaviors that Lee engaged in, but focuses instead on indicting laboratory security practices more generally. The tenor of Trulock's account is best capture by his own quotation of the Redmond report:

> "DOE is a large organization saturated with cynicism, an arrogant disregard for authority, and a staggering pattern of denial. Even after President Clinton issued a Presidential Decision Directive *ordering* that the Department make fundamental changes in security procedures, compliance by Department bureaucrats was grudging and belated."

We are left to conclude that, while the question of Wen Ho Lee's guilt or innocence is in the end finally unknowable, that question is probably moot. The larger questions should address instead what the appropriate measures are for enhancing national security, either via openness and

hopefully from that increased technological development as the labs seem to prefer, or via control of information if some mechanisms of enforcement can be enacted given an organizational culture that has historically developed in a very different direction.

The Lee case, shaped as it was by the context of DOE rather than exclusively intelligence-oriented organizations, exemplifies some of the issues in espionage rhetoric. The interdependence of the media, legal, and internal discourses sets up expectations that are difficult to alter because of their reinforcement in other channels. The accusations seem to take on a momentum of their own, not because of any intentions on the part of any individual, but because once set in motion the espionage charge attracts such a large amount of attention, and espionage charges habitually follow a set pattern. Because of the role of espionage as a political crime, preservation of the political status quo tends to mean that more often than not trials end with a dramatic denouncement of the spy. The Lee case is unusual in that rhetorical intervention in the three interdependent discourses was possible and largely successful. The judge's dramatic turn-around, from believing solitary confinement without bail was essential to believing that an apology was appropriate, was possible because the intertwining of the discourses eliminated some of the elements of secrecy that in other cases serve as support for accusations of espionage.

"Treason doth ne'er Prosper; What's the Reason? For when it Prospers, None dare call it Treason!" Sir John Harington, *Epigrams of Treason*

Robert Hanssen and the Excitement of Espionage

The FBI has only had three spies from within its ranks over the course of its seventy-five year history. The FBI is both older than the CIA, and has had fewer spies than its counterpart intelligence agency. The first, Richard Miller, was arrested in 1985, the Year of the Spy. The second was Earl Pitts[42], who was caught in 1996 when his estranged wife turned him in. The third was Robert Hanssen, who was arrested in 2001 after twenty years of selling secrets to the Russians. Robert Hanssen is the most damaging spy in the FBI's history. Hanssen had sold to the Russians twenty-five floppy disks with classified information, and numerous other classified original documents. Hanssen is unique in that he rarely if ever photocopied documents to pass to his handlers. He sold them what he was certain would not be missed, or occasionally asked them to return a document after reviewing it, or he duplicated electronic files. For example, in hard copy he gave them a document that he himself had prepared, a study on the possibilities of a mole penetrating the FBI. Another time he gave them an NSA document reviewing future needs for SIGINT, which he required that they return to him. In electronic format, he accessed files from the FBI, the CIA, the State Department, and the President's cabinet. He was able to sell files that he had no legitimate access to, because of poor computer security practices. The introduction to one of the biographies of Hanssen includes a quote from an FBI agent stating that "Hanssen is the worst spy since the Rosenbergs." The quote should sound familiar, for the same claim was made in relation to the Wen Ho Lee case.

So what had Hanssen done that caused a fellow FBI agent to condemn him in terms that evoke the death penalty? One answer is that Hanssen is an affront to the pride of the FBI. He is only the third traitor from their ranks, and the first one that has received significant publicity. He

spied for twenty years, the longest spying career of any U.S. traitor, though other countries have been vulnerable to much longer careers among spies. In the Lee case, the official making the Rosenberg comparison was from the Defense Department, which positions him as an outsider and hence a more objective perspective from which to analyze relative damage, and also arguably is the position from which "national security" can be best judged among any single government agency. The FBI agent is making the comparison because of his position within the agency, and is perhaps making the claim hyperbolically. Perhaps all he really means to say is, "this is serious stuff, you should read this book and be concerned."

The other way to attempt to answer is to assess the impact on national security caused by Hanssen. To do so, we will turn to the legal documents and court case surrounding the Hanssen trial. The trial ended with a plea bargain, in which Hanssen was sentenced to life in prison and agreed to cooperate with the damage assessment, in return for his wife receiving his FBI pension. The plea bargain was arrived at only after a year-and-a-half of negotiations. It might seem surprising that the plea bargain was only reached after such a long period of negotiations, given the strength of the government's case and the severity of the sentence agreed upon.

The prosecution's case against Hanssen was exceptionally strong. The original documents had been obtained from the Russians. The Russian file had included a tape of the one phone call between Hanssen and the KGB, and also included a plastic bag with Hanssen's fingerprints on it. The file also contained every message sent between Hanssen and the KGB, and a description of every document, though not in all cases the document itself. After receiving the documents, the FBI and Department of Justice had taken a gamble: they left him free in an attempt to apprehend him in the act of espionage. Catching the spy in action would provide much stronger evidence, particularly in combination with the evidence of the long history of espionage documented in the files. Hanssen was "promoted" to a position created to keep him busy and hopefully unsuspecting, but not provide him with any access to important classified

information. The gamble was surprisingly successful. Hanssen was fully aware of the meaning of his new position, and wrote to the Russians that he suspected a new mole in their midst because of the "promotion." Yet he chose to continue selling secrets, which he stole off of the computer network using passwords, sometimes his own and sometimes those he hacked. The FBI arrested him red-handed in February of 2001. John Ashcroft, the Attorney General at that time, favored seeking the death penalty given the strength of the prosecution's arguments and the favorable venue, for Virginia juries are frequently willing to sentence criminals to death, and the case would be tried in the Virginia courts near where Hanssen had lived.

Ashcroft's assertion that he would seek the death penalty was made publicly in spite of the fact that the representatives from the CIA and FBI both preferred to seek a plea-bargain that would ensure Hanssen's cooperation. Hanssen's lawyer, Plato Cacheris[43], was quick to point out that Hanssen was probably not eligible for the death penalty in this case. Death for espionage had only been reinstituted in 1994 in response to the Ames case, and much of the government's evidence addressed espionage that occurred before then, and it is illegal to convict someone of a crime if it was not illegal when the crime was committed or to apply a penalty that was not eligible at the time the crime was committed. Also, the death penalty is only applicable for espionage of very specific sorts. The espionage must have passed to a foreign power information relating to nuclear weapons, military spacecraft or satellites, early warning systems, major weapon systems, battle plans, or "any major element of defense strategy." An argument might be made to the effect that Hanssen had compromised secrets related to "major elements of defense strategy," but only this last category might possible provide eligibility for the death penalty.

Which still leaves the question unanswered, why did it take so long to reach a plea bargain given the strength of the case, even if the death penalty could not have been sought?

One way to answer this question might be to consider the nature of espionage as a crime of communication.

ESPIONAGE AS COMMUNICATION

The laws regarding espionage implicitly assume a transmission model of communication. The theory of communication is not, of course, stated in any explicit format, but we can understand a great deal about how "communication" is conceived by studying what gets regulated, how it gets regulated, and how those regulations are enforced.

To review briefly, the important characteristics of a transmission model of communication focus our attention on communication as information. Other characteristics include an emphasis on a sender and a receiver, with the roles alternating rather than simultaneous. The channel of communication is of interest because it generates "noise," which can be understood and detected in terms of imperfections in the communication when it reaches the receiver. Espionage laws can best be understood if we presume precisely this model of communication. The "communication" gets reified as a "thing," and a very specific type of thing. This thing can be controlled, it can be possessed, it can be given to others, it can be damaged, and above all it can be detected. Notice that the metaphors we use when we talk about espionage are about "giving" or "selling," not "sharing," not "reproducing," and certainly not "creating." These verbs signal that this activity, this illegal communication that is labeled espionage, deals with a fixed quantity.

This fits perfectly with the transmission model of communication. The sender, or spy, possesses this valuable commodity. S/he uses a channel of communication, and the channel is the aspect that most spy novels seem to obsess over. How does the message get passed? Are there elaborate codes, that can be broadcast via some segment of the electromagnetic spectrum such that even though they're being broadcast only the intended recipient can get the information that's been encoded and hidden? Are there "dead-drops," or secret locations where first sender

and then receiver can go to interact asynchronously? Are there clandestine meetings, risking everything because of some felt need for face-to-face communication? Any channel presents its own vulnerabilities, any choice is fraught with different kinds of risks. Once a channel of communication is established, relevant issues of "noise" would include the various ways in which an investigator could perhaps find evidence of this illegal communication, this ongoing espionage. To actually interrupt the act of communication first-hand is the goal for every espionage investigation, because without it prosecution becomes difficult.

There is a final requirement for understanding the definition of communication that undergirds our understanding of espionage. That which gets communicated, in order for it to "count" as treasonous communication, must be considered truthful. If that which gets communicated is believed not-true by the individual doing the communicating, or by the society which is passing judgment regarding the communication, then whatever else it might be it's not an example of espionage. Indeed, often the communication of untruths is celebrated by the originating society. When the engineers at NASA deliberately included an untruth regarding the specifications of the materials for heat-shielding the shuttles on their web-page, they were certainly not accused of espionage. The "information" being communicated satisfies all of the other criteria: an enemy country was the recipient (as were many friendly countries, who were also taken in by the deception–indeed the British were at one point forced to seek our aid in diagnosing why their rockets were not surviving re-entry, and we had to reveal to them that it was because they were using the false data provided on NASA's website), the topic was one which was militarily sensitive and officially declared secret, and no public or official approval for engaging in the communication had been obtained. But because that which was communicated was false, the deception was praised rather than prosecuted by the Americans when it became publicly known because the Russians had a series of embarrassing failed re-entry experiments. Thus the layers of deception that are the core of espionage begin. The

recipient country must be suspicious of every communication, because the truth or untruth of the shared secret makes all the difference. Only true secrets have any value to the recipient, while to the originating society false secrets shared are a victory in the world of counter-intelligence. This strategy is called "disinformation."

The layers of deception build upon one another, creating a communicative situation that is paradigmatic of a problem that all communicative interactions face. How do we establish truth, and how do we assign value to a communication whose truth cannot be perfectly verified? The layers of deception create a "wilderness of mirrors," to use the phrase coined by Angleton, the CIA's first master of counterintelligence. And in that wilderness, what tangled webs we do weave! Passing that judgment, on communications which must be kept hidden and so cannot be verified or falsified using community consensus the way scientists routinely proceed, is the central problem that intelligence agencies face. Failure to correctly judge, and assuming too many false-positives (that is, assuming that a communication is true when in fact it is false) leads to disadvantages for the society as a whole, an inability to correctly decide what actions should be taken or what intentions other nations hold. Failure to correctly judge, and assuming too many false-negatives (that is, assuming that a communication is false when in fact it is true) leads to missed opportunities and increased risks for the entire society, and unnecessary risks to the originator of the communication–sometimes even loss of life if the communication is not kept hidden.

BETRAYING THE TRAITOR

Thus there is a premium on attempts to ferret out the true spy from the false intelligence agent. No individual's communications can be taken at face value. All information must be tested against the totality of other information taken to be true. And the search for originators of true information is relentless–in the ranks of other country's intelligence agencies, but even more ruthlessly in the ranks of one's own intelligence agency.

In 40% of all espionage cases, the spy is discovered through the betrayal of another. This number is calculated on the basis of the Defense Security Service's survey of Recent Espionage Cases. Cases were coded as "betrayals" if the spy was *discovered* through the testimony of a defector, a co-worker or partner-in-crime, a friend or family member, or through turning themselves in. In the remaining 60% of the cases, the spy was discovered through actions of an investigating agency, or in a few cases the method of discovery was not specified. The betrayals that reveal spies take a variety of forms. We recruit an agent from the agency for whom they are spying, and that agent has knowledge that he shares with us. Or a family member or friend learns something about the spy that indicates their illegal activity, and the family member or friend provides that information to an official in a position to act upon it. In some cases, a spy is caught because another member of his or her "spy ring" is caught, and sells the names of accomplices in return for a lighter sentence. Occasionally, a spy will also turn himself in. Even in cases where a spy is not initially discovered through betrayal, successful prosecution almost always depends upon the testimony of witnesses, so that all told far more than half of all espionage cases are dependent upon informers such as these. An additional 20% percent of espionage cases are discovered through the use of "sting" operations, whereby a government official (usually FBI) poses as an agent of a foreign government and offers money in return for classified documents[44]. The method is deceitful, though not a betrayal since there should have been no expectation of loyalty. This means that in the majority of cases, a spy is not caught through clever investigative practices, but is caught rather because the web of lies and deceit that a spy weaves entraps him or her. Those who betray, are betrayed in turn.

Such was the case with Robert Hanssen. The important break in the case came when a still-secret and unnamed Russian KGB agent defected to the United States, and brought with him a number of the active case files in use by the SVR (after the fall of the Soviet Union, the KGB did not simply vanish, it morphed into a successor agency known by its abbreviation, SVR)[45].

The FBI had known by then that there was a mole still active in one of the intelligence agencies. During the debriefing of Ames, it became very clear that while he had sold more secrets than even he could remember, there had been operations compromised that Ames could not possibly have known about. The defection of this Russian and his files raised the stakes for Hanssen, who could have no way of knowing whether or not information that could be used to identify himself would be found in the files. He had carefully avoided allowing the KGB to learn his true name, an unusual agreement for the wily KGB to go along with. Hanssen's anxiety level must also have been raised by the fact that Patricia Galey, the stripper upon whom he had lavished gifts and attention, had been arrested for cocaine use, and could very easily say something that would draw attention to Hanssen's wealth. Hanssen had scrupulously avoided spending more than his regular salary would seem to permit on his house or car or family or travel, and had asked the KGB to provide diamonds instead of cash when possible, so that his personal finances could not have been used as part of an espionage investigation. He had been peripherally involved with the investigation of Ames, and was familiar with the kinds of clues the FBI investigators would be looking for.

UNDERSTANDING MOTIVATION

The FBI itself deserves little of the credit for finally stopping the twenty-year espionage career of their Chief of Soviet Counterintelligence, the position Hanssen had held for much of his career at the Bureau. Hanssen's career–both its rise and its fall–can best be summarized in the words used in the sentencing memorandum issued in evaluating whether his plea bargain should be accepted:

"Robert Philip Hanssen is a traitor. For all the words that have been written about him, for all the psychological analyses, the speculations about his motivation, and the assessments of his character, this is, at the end of the day, all that really warrants being said about Hanssen. He

is a traitor and that singular truth is his legacy." (05/02/02, Criminal Docket #01-188-A, U.S. Eastern District of Virginia Court, Alexandria Division)

Although this sentenced brushes aside the issue of motivation, a great deal of speculation about his motivation and assessment of his character have dominated the rhetoric which has surrounded the Hanssen case. Motivation is a central term for rhetorical analysis. Indeed, Kenneth Burke pointed out in his 1935 book Permanence and Change: an Anatomy of Purpose that "motivation" is one of the key organizing principles for entire systems of ideology. Motivation reappeared as a key term in both his A Grammar of Motives, where it is one of the five elements of the pentad for giving accounts of action. Motivation for Burke may or may not have to do with the psychology of the actor himself or herself, but it has everything to do with the key terms that are used to make sense of that actor's behaviors. Thus for example a Freudian analysis of motivation reveals a great deal about the perspective of the analyst, and the rhetoric of the analyst's account-giving. It reveals assumptions about the analyst's understanding of the intentions and thus relations of all other human beings. The Freudian analyst views human motivation as essentially non-rational, driven by animal instincts, and fundamentally deceptive. An alternative account of motivation, such as that provided by a Marxist, would create a rhetorical vision with the audience as essentially economic. For Burke, our accounts of the motivation of others and our accounts of our own motivation are equally perspective-laden, hence rhetorical. Both types of accounts are the product of the values espoused by their own social group. "One school's reason is another school's rationalization," as Burke says on p. 20 (2nd edition). The key to being persuaded by an account, Burke argues, is the ability to identify with the vocabulary of motives being used. Accounts of motivation are persuasive in that one vision of motivation can replace alternative explanations, and then perhaps go on to become the dominant lens through which we understand the behavior of others. "Any set of motives is but

part of a larger implicit or explicit rationalization regarding human purpose as a whole," Burke says[46]. (p. 26)

Motivation is the central theme of most espionage writing. Intelligence practitioners, scholars, and fiction writers & readers all construct careful theories of motivation. Consider for example, Eco's analysis of Ian Fleming's James Bond novels, a prototypical example of the genre of espionage writing. Eco is analyzing the variations of the Bond theme, and the interesting common thread across all the Bond novels is the motivation of the characters. Bond represents the motivation of the Westerner–money, ideology, and sex. The villains consistently are represented as a stereotype of a subgroup, and their motivation is deformed in the same way that each of the villains in their physical description are deformed. The motivations rely also on stereotypes regarding other groups. We assign greed to the Jewish villain, lust for power to the Russian villains, an excess of anger to the African villain, and so on. What Fleming is doing and Eco is highlighting is a scheme of motivation in which individual motivation is ascribed to the group's influence, and/or to the villain's position as outcast from his[47] group.

Typologies of motivation are also popular in non-fictional accounts of espionage. Intelligence practitioners develop typologies both to figure out how to induce an intelligence operative to become a double-agent, and to prevent or locate traitors amidst their own ranks. The most influential of these practitioner-driven typologies was developed by the KGB. The typology is known by its acronym: MICE. Spies can be motivated by money (or other resources–the U.S. has been known to use the promise of citizenship, or employment, or housing, among other useful bribes); or by ideology (not always pro- or anti-Communist–the Soviets for example were several times able to use racial resentments to motivate U.S. agents to sell secrets, and in other cases spies were seeking to secure "world peace"); or by coercion (sexual coercion, or honey-traps, are the most widely known, but blackmail based on criminal acts or any potentially embarrassing information is possible and has been attempted); or for

excitement or egotism (the Soviets were particularly skilled at subtle flattery–capitalizing "You" in correspondence with Hanssen, for example, or giving medals or other awards at secret ceremonies). The KGB typology shaped Soviet practices in predictable ways that in turn shaped U.S. counterintelligence practices in ways that are still dominant today.

The adoption of this typology has had a variety of consequences. For example, U.S. counterintelligence is less able to deal effectively today with, for example, the Chinese strategy. Chinese intelligence agents reputedly delegate specific tasks to numerous of their citizens, for example "tasking" their exchange students and visiting scientists. These citizen espionage agents ask very specific, seemingly-innocuous questions of every single individual encountered. The U.S. counterintelligence strategies that have developed based on Soviet intelligence measures are also not effective to deal with a strategy of systematic disinformation designed to alter the perception rather than the motivation of an agent. Thus the arguments of John Walker Lindh regarding his beliefs while working for the Taliban are consistent with an intelligence strategy widely used by less-wealthy nations, which U.S. agencies have developed no easy way of countering. Our Constitutional protections of free speech make it impossible to control the dissemination of disinformation, and the reliance on informal, interpersonal channels of communication for such information make it difficult to even track, let alone control or counter. There are periodic attempts to do so however. In preparation for war in Iraq, President Bush re-opened a division of the State Department dedicated precisely to countering disinformation strategies, called the Office of Misinformation/Disinformation Counter Reporting. The office had been closed, following arguments that the best way to respond to Soviets deliberately spreading untrue stories was to ignore them, not bother dignifying them with a response. Today the office employs a staff of three, whose responsibilities include crafting responses to stories that are identified as deliberately disseminated, widespread falsehoods.

The most thorough account of motivation for espionage is that of Frank Hagan, in his 1989 book Espionage as Political Crime. Hagan develops nine categories: mercenary, ideological, egocentric, buccaneer, professional, compromised, deceived, personal problems, and professional. Hagan's work is important because the typology he developed became dominant in scholarly work, and also because it provided a much-needed antidote to a prior widespread misconception[48]. Previously, spies had been characterized as "sad cases," (Bulloch, 1966, Akin to Treason) the idea being that every case of espionage was characterized by a "fatal flaw" in the spy. The argument is similar to the characterization of classical Greek Tragedy. In Greek Tragedy, the downfall of the erstwhile-hero is brought about by Hubris. In Western literary accounts today Hubris is less common a flaw than greed or stupidity, but the action of the plot remains the same. The strategy, then, is to make sure that intelligence agents (G-Men, in the FBI's classic portrayal of the type) are strong, resourceful, all-around-great-guys. The FBI went to significant lengths to try to inculcate this characterization of their intelligence agents, with Hoover personally taking a hand in the development of an early television series (Barnouw, 1978)

Any assumption that all spies are "fatally flawed" also makes it less likely that a spy will be successfully identified. To serve as a useful guideline (in some sense all humans are flawed, but then the maxim can't help narrow down a list of suspects), the search for "fatally flawed" individuals is likely to eliminate any individual that the investigator likes as a person. Thus those who are most likely to have access to information, legitimately or through corridor-gossip, are least likely to be suspects.

One problem with every typology of motivation is the same: it leaves open the question of why people with similar "flaws" or weaknesses do NOT become spies. In other words, why does one individual with debt problems, or with deviant sexual preferences, because a spy while another with a similar background does not become a spy? When the total number of individuals

with access to classified information, and who are therefore potential spies, is compared with the total number of known spies, the percentage who spies represents less than one-hundredth of a percent. The number of "fatally flawed" individuals is significantly broader than that no matter how we define that term. In the case of Robert Hanssen, an additional problem with typologies becomes apparent: each assumes that we can come to understand the psychology of another human, and that the accounts people give of themselves should be credited. The reasons why a spy claims to have done what s/he did might tend to fall generally into neat typologies because those are the socially understood and –not exactly accepted, because espionage is frowned upon as outside of the realm of acceptable behavior-- but at least given credence as believable, sufficient explanations so that we will rest easier. Walter Fisher's theory of narrative coherence, and in particular character coherence, can provide some insight as to why there is such a powerful desire to understand the motives of spies. We rely on characterological coherence in order to fit other humans into narratives that we can find both comprehensible and believable. A character whose motives remain incomprehensible, or at least inexplicable through any of the narrative devices that we have learned through previous narratives or through experiencing our own lives as narratives, is not a believable character. In order to reconcile believing in the espionage and the betrayal that must represent, we must summarize the spy's motives in a way that both casts them as the villain in the story (otherwise we have to reevaluate whether the espionage really caused any serious harms) and yet also casts them as comprehensible, in some sense fellow human beings. The balance of comprehensible yet reprehensible is the heart of the challenge in writing a good spy novel, or in constructing a narrative that is coherent and has fidelity out of the layers of mystery involved in a real-life spy case.

The challenge with the Hanssen case is to achieve that balance that will enable us to understand his motivation. Hanssen's motivation is not fully understood (perhaps not even by himself), and cannot be forced to fit neatly into any of our typologies. This is particularly

striking, given that there are more books devoted to the Hanssen case than any of the previously considered cases, though the newspaper coverage has not been as extensive. There are currently six books detailing the Hanssen case, while Lee has three books and Ames has four. The difficulty in understanding his motivation might explain why the Hanssen case is the only one that was in fact turned into a television movie. Plans were initially made to shoot a Wen Ho Lee mini-series, but after the dramatic real-life ending those plans evaporated even before any casting decisions were made. Two televised interviews with Aldrich Ames were broadcast, but no fictionalized account was ever adapted to audiovisual format. Hanssen's story was scripted, cast (with William Hirt playing the role of Hanssen), and broadcast in mid-November of 2002.

Explaining Motive in terms of Greed

The easiest explanation for Hanssen's betrayal is that he was motivated by greed. The Russians gave him $600,000, and had supposedly set up a bank account for him in Russia with an additional $800,000. Hanssen also requested diamonds from his handlers, and he received several. He was enough of a gem connoisseur to distinguish one or two of them as flawed, and returned them with a request for an equivalent value of cash instead. Why diamonds? Because Russia is well-known for its high-quality diamond mines, and because the diamond trade is well-known as being one of the least-regulated. It doesn't even really make sense to speak of a "black market" in diamonds, because the entire diamond market is so porous and saturated with illegally-acquired gemstones. The preference for diamonds was clever in the sense of being difficult to trace, but foolish in the sense that it was so unusual. The KGB had to go outside of its normal channels to procure suitable diamonds. The uniqueness of the request and the difficulty meeting it meant that more KGB agents knew about the novelty of paying a spy with diamonds than would have known about cash. Long before a defector brought the file related to Hanssen, the FBI had known that there was a diamond connection involved with their mole hunt, from conversations with non-KGB defectors.

The trouble with explaining Hanssen's motivation in terms of greed is that he did not spend any of his ill-gotten gains on himself, and his lifestyle was not improved by the additional cash. Most of the money that got spent was lavished upon the stripper whom he claimed he wanted to redeem. Additionally, some small amount of the money was spent to help finance his children's private educations. But Hanssen's wife remained unaware of his espionage profits in spite of the fact that she was on the lookout for such signs, since she knew of an earlier attempt at espionage that he had committed. And the FBI, in reviewing his financial records, never found anything out of the ordinary. He and his family lived for the most part within the means that his FBI analyst's salary provided, with perhaps occasional help from relatives, since Bonnie's family was relatively well-off. If greed were his motivation, why did he not spend his illegally-gotten money? His familiarity with the Ames case could perhaps justify his caution in spending, but then the question remains of why he chose to engage in espionage that he could not enjoy the benefits of. The other difficulty with attributing motivation to greed is precisely because we know he was familiar with the Ames case, and with the fact that the Russians had been known to purchase secrets for much higher prices. Ames garnered roughly three million dollars, while Hanssen spied over a long period for less than a fifth of that price. If greed were his primary motive, why did he not demand the profit that he knew the market would bear? He did not even seem to care whether he was given the money he knew his secrets were worth. In his first message to the Russians, he referred to documents he would be sending as "... worth consideration in the amount of $100,000." The Russians left him only half of that, $50,000. Hanssen's next communication praised the Russians' decision. "As for the amount, it is better not to include sums larger than $50,000, for reasons of difficulty determing (sic)[49] how to hide it."

Explaining Motive in terms of Religion

Another possible motivation is ideology. Hanssen's religious beliefs have been blamed as motivating or at least enabling his espionage. Hanssen was Catholic, but more specifically he was a member of Opus Dei. Opus Dei was founded by Josemaria Escriva, a Spanish priest who was canonized in 2002. Since its founding in 1928, the organization has grown to include roughly 80,000 individuals in 80 countries, and is recognized by the Catholic Church as the first "personal prelature" (in contrast to the usual hierarchies within the church, which are usually geographically defined). The defining belief of Opus Dei, which means "Work of God," is that every activity one engages in should be dedicated to attempting to become a saint. In Pope John Paul II's address on the occasion of the founder's canonization, he explained the focus as, "For every baptized person who desires to follow Christ faithfully, the factory, the office, the library, the laboratory, the workshop, the home, can be transformed into places for an encounter with the Lord. Daily activities, even in their seeming dullness in the monotony of actions that seem to be repeated and always the same, can also acquire a supernatural dimension and become in a certain way transfigured." This emphasis on individual personal holiness can have different meanings to different individuals. Bonnie Hanssen interpreted it as a reason to withdraw from contact with non-Christians and spend her time in contemplation, teaching children, and prayer. Bob Hanssen seems to have interpreted it as justification for selling the most deadly secrets he could get his hands on: the contingency plans for government if all of the Washington leadership gets wiped out at once, the nuclear target second-strike plan (in case we get decimated by a first-strike nuclear attack, but have some remaining weapons that escaped the devastation), and the intelligence community's assessment of Russia's military capability. Some of the secrets selected might be considered those most likely to encourage the Russians to do something drastic, something that would trigger Armageddon. This apocalyptic emphasis is not inherent necessarily in the teachings of Opus Dei, but the awareness of the Second Coming and the end of the world is present even in the public discourses of Opus Dei. Again from the Pope's address

upon canonization of the founder, "By sanctifying one's work in accord with the norms of objective morality, the lay faithful contribute in an effective way to building up a society that is more worthy of man. They set free creation that groans and suffers waiting for the revelation of the sons of God (cf. Rom 8,19-22)." Hanssen might have believed that selling these secrets would assist in reaching this goal. When he began his espionage, it might have been less obvious that the Soviets were not likely to have any desire to begin Armageddon regardless of what secret knowledge they gained about U.S. contingency plans. The secrecy Hanssen experienced as part of his intelligence work would have been reinforced by the secrecy of Opus Dei. Former members of Opus Dei have formed a support group called ODAN (Opus Dei Awareness Network), and have accused the group of being a cult. The accusations are in part based on the extent to which secrecy is maintained and members are expected to engage in private rituals of self-mortification. Opus Dei's officials deny that the group is "secretive," insisting that the perception is based on the fact that practicing personal holiness demands absolute humility, and that to discuss any individual's efforts dedicated to God is to diminish them. "The spirit of Opus Dei encourages members to make these daily tasks worthy to offer to God . They try to practice Christian self-denial, especially in small things - at work, in family life, putting others first, paying attention to detail, and so on." (www.opusdei.org)

Regardless of whether his religion influenced his decision to begin spying, it certainly influenced his decision to continue. He believed in the sacrament of confession, where by confessing his espionage he would be absolved of all sin in relation to his espionage, and in relation to his sexual peccadilloes. He informed his psychiatrist later that he had confessed his sins regularly, throughout all the years of his espionage. The Hanssen's jointly believed in the potency of confession for wiping away sin. In 1979 when Bonnie discovered her husband's first attempt at espionage, she insisted they go jointly to confess to their priest. The priest required that he give the money to Mother Theresa's charity organization. But the priest did not require

him to confess to his employer, or impose any other personal penance. The pattern of Hanssen's later espionage can perhaps be seen here: give the proceeds to charity and espionage can be forgiven.

Certainly, it seems as if religion played an important part in Hanssen's life, since he attended church every evening and sent all of his children to Opus Dei private schools, and since he did indeed confess his crimes. His involvement with Patricia Galey, the stripper, was rationalized as an attempt to save her soul. He proselytized at work to the few agents who interacted with him socially. On the other hand, religion might not be a believable explanation. His church gave Hanssen no explicit encouragement, and at confession the priest did tell him it was wrong and he must stop doing it. And for a while Hanssen would stop. One reason he was not caught in spite of the fact that his espionage career spanned twenty years was because most of the time, he was not actively engaged in espionage. Only during three periods, generally as short as two years each, did he interact regularly with the Russians.

Explaining Motive in terms of Insanity

A third possible explanation of his motive was some variant on insanity, probably multiple personality disorder. Three psychiatrists who have interviewed him prior to his sentencing have come to similar conclusions, and one considered the trial sufficiently unjust to require him to break the usual patient-therapist confidentiality agreement and speak publicly about Hanssen's mental condition[50]. Evidence of split-personality disorder can be found in the fact that he often seems not to have remembered what he himself had done. He denies remembering some of the unpleasant interactions with his father that others in his family witnessed. For another example, one source of evidence found and used to support conviction at his trial included recordings from his bedroom which showed him hiding one of the packages from the Russians. He had installed the camera in his bedroom himself, in order to record and transmit video of him and his wife having sex. His behavior with his high-school friend Jack

Hoschouer included visiting strip-clubs, fantasizing about partner-swapping, and ogling, sometimes harassing, women on the streets that they passed. All of these behaviors would seem to be anathema to the highly religious persona he cultivated in all other relationships. The diagnosis also fits the profile of those typically found to have MPD. His childhood included physical and psychological abuse by a father who constantly belittled him, but whom he alternately avoided and tried to emulate, including his career choice in law enforcement. His dad had been a Chicago police officer doing wiretaps and surveillance. An interesting parallel is the fact that Hanssen senior had supposedly burned his files, knowing that it would mean his forced retirement, but also knowing that some of the investigations he had files on were illegal and would bring shame on the whole department. Surely this story would have come out during the background investigation before hiring Hanssen, so it seems interesting that this example of a warped sense of loyalty did not raise any red flags in his security clearance.

The problems with this possible attribution for motive are twofold. The first difficulty is that if indeed he was to considered by experts not mentally competent, or if there was even a good argument to be made, why would he not use this defense in his trial? The short answer is that he refused to consider attempting it. This is one of the reasons why his first psychiatrist chose to violate doctor-patient confidentiality. Why did Hanssen refuse? Pride, perhaps, or perhaps because the risk associated with attempting such a defense and possibly not succeeding, seemed a greater risk than the plea bargain the government proffered. The other problem with attributing his motive to a psychiatric disorder would have also made such a defense risky. Hanssen was a remarkably canny spy, who covered his tracks as carefully as any sane man could. The FBI would never have found him had they not been able to purchase the evidence from the Russian defector, in return for seven million dollars. Seven million dollars is a high price to pay for information about one spy, though today by comparison the price might not seem high, given that we have paid 27 million for information about one leader of al-Qaeda.

Explaining Motive in terms of Employment Problems

Another possible motivation, the one that the television movie and majority of books seems to have favored, was disgust with the intelligence system, both in our country and in Russia, and an arrogant belief that he was smarter than anybody else in the system or indeed the system taken as a whole. He could beat the rotten intelligence system at its own game. Here we can see echoes of Ames' motivation, but Hanssen never managed to articulate his motivation as intelligently as Ames was able to critique the system and what was wrong with it. Certainly, Hanssen's case points to problems within the intelligence system, particularly the computer system that he was able to hack so easily. But while his case points to flaws, he himself espouses a continued belief in the importance of intelligence work and pride that the FBI is the best in the business. Dissatisfaction with working conditions–usually due to a failure to get promoted or a reprimand believed to be unfair–is a common motivation among espionage cases that have been caught. But Hanssen had been promoted, and was viewed as a highly-valued agent by his superiors, so disgruntlement seems a problematic motivation to assign. The attempt to assign Hanssen's motivation to personal issues, or "ego" in the acronym of intelligence agencies, is problematic in another sense. His willingness to out-spy both the FBI and the KGB can be framed as arrogance, a belief that he can outwit both intelligence agencies. But his Russian handlers, in the communications sent to him with the payments, seem to frame his motivation as a deep insecurity instead. The letters are full of flattery, mostly subtle, sometimes less so. The flattery could be as simple as, when providing instructions, "We are sure You remember..." or as clear as "Your superb sense of humor and sharp-as-a-razor mind, we highly appreciate both." The Russian attribution of motivation is perhaps the most persuasive one, in that it is perhaps one of the reasons why Hanssen continued spying. It is persuasive in the sense that rhetoric is often judged on the basis of its success, and the Russians did succeed in retaining

the services of Hanssen as a spy. Whether there is a valid cause-effect relationship between the rhetoric used by the Russians and the fact of Hanssen's continued spying is a question that cannot be answered. And it is difficult in the rhetorical vision of most Westerners to conceive of motivation as being both simultaneously arrogance and insecurity, though in rhetorical systems more accepting of paradox perhaps this would be the dominant, satisfactory attribution[51].

Contrasting Examples for Simplifying Motive Explanations

Perhaps we should not be surprised at the complexity of assigning motive in Hanssen's case. Reflecting on our own experiences in life, how often is any major decision based upon one dominant motive? And how often do we understand our own motivation? Often we can construct a rationale in hindsight, but the story that gets told retrospectively is a device for imposing order and making sense that the original series of events did not necessarily possess. Perhaps instead of wondering how to assign motive in the Hanssen case, we should rather be questioning why in other cases of espionage motive seems to be assigned so simply and to remain clear even when a case takes numerous twists and turns.

Consider for example the Lee case. Motivation was established before the suspect was even identified. The motive was assigned as ethnic loyalty, and then later as greed in the sense of seeking profitable employment. Lee did not proffer an alternative explanation of motive, because he denied having spied. In rhetorical terms, Lee was emphasizing the stasis of conjecture. For Lee to have argued motive would be to allow a shift to the quality stasis, arguing whether the act was justified, which would have entailed admitting that an act (espionage) had occurred. Therefore Lee could not contest the prosecution's construction of his motivation. The account of Lee's motivation therefore remained a highly simplified vision based on ethnic loyalty.

Ames' case is more interesting for considering alternative motivation constructions. Retrospective narratives have always left Ames' motivation as simple, easily-understood greed. It fit well with other aspects of the case. Ames was caught because of his lavish lifestyle, and in comparison to other spies Ames was paid more than anyone else. Ames himself accepts this construction of motivation, and plays up his feeling of desperation for money when he is interviewed publicly. But we could consider alternative constructions of motivation. Ames could as easily be said to have spied out of resentment at his lack of advancement at work, or for ideological reasons like disillusionment with the current practices of intelligence. Better yet, we could step outside of the typology of motivations and explain Ames in terms of his drunkenness. An alcoholic is likely to make poor decisions, which upon sober reflection s/he is unable to construct any rational-sounding motivation for. Or more likely, motivation consists of some combination of these known and other unknown and perhaps inarticulable factors, just exactly as in Hanssen's case. Why, then, do we fixate on explaining Ames in terms of greed? Two possibilities I'd like to suggest. One is American ideology. Our capitalist ideology inclines us to explain everything in terms of market value when we have the option. The other is narrative form. Ames is, and must be, cast as the villain in stories told publicly. Greed is more clearly a villainous motive than resentment over lack of recognition or disillusionment with the goals of one's work. Why this should be the case probably traces back to the first explanation. The important consequence though is that by simplifying motive as greed we reduce the tendency to empathize with the villain of the story. The story gains further simplicity by having a clear heroine in the person of Diana Worthen, the betrayed friend who first named Ames a suspect. Ames' later utility in helping with other espionage investigations and recommending changes for the congressional subcommittee investigation, which finally gives him a role to play other than simply that of villain, has created more recently a rhetorical situation in which alternative constructions are possible.

In the end, Hanssen's case cannot be simplified in the way that other espionage cases can, because none of the attributions of motivation are satisfactory for narrative purposes. We are left without an easy ascription for the case, and my guess is that this is why coverage of the Hanssen case has been different than any of the other cases considered. It could account for why the type of coverage which the case did receive is qualitatively different, and relies on different channels of communication. It is, in short, a mystery, and as such it intrigues.

CRITIQUING CONTRASTING ACCOUNTS

Television as a Constraining Medium

The television biography of Hanssen provides an account of motive that works sufficiently well as a narrative and is particularly well-adapted to its medium. The broadcast was aired over two weeks. The first half begins in Russia, with the actors speaking Russian and subtitles appearing in blue at the bottom of the screen. Why? Do we still view Russia as menacing enough that this counts as an appropriate way to set the mood for a spy-thriller? Is it striking enough to get attention in spite of the fact that in general American audiences are known to have little patience with having to bother reading subtitles? The newspaper accounts never emphasized that it was the Russians he sold secrets to, presumably because the writers judged this approach to be an ineffective strategy for establishing the harms to our society today. That is to say, emphasizing the role of the Russians as enemy, in order to illustrate the harms of the case, was not an alternative the newspaper accounts chose, in contrast to the televised discourse. Newspaper accounts of the Lee case, by contrast, or the Ames case only six years earlier, both discussed at length what the recipient country could do with the information gained through the espionage. The discussions of China, in particular, represented a significant portion of the early articles regarding the Lee case. Hanssen articles, by contrast, rarely mention Russia in more than one or two sentences. The television movie version, however, highlights the Russian connection.

The primary focus of the movie was on the question of motivation. How does one address motivation in a television format? Given that motivation is understood by the average television viewer as an internal, psychological state, visuals to accompany the assignment of motivation seem problematic. And indeed, the movie's greatest flaw is its inability to satisfy understanding of Hanssen's motivation. The movie early on uses numerous shots of Hanssen looking into mirrors, or reflected in the windows of buildings, or other mechanisms for doubling his image, in which he talks to himself. The voice inside his head is meant to sound slightly different than his spoken voice during conversations. This should then cue the audience that the dialogue following is internal, and hence represents his reflections and sense of motivation. The problem is, the voices are not significantly different. The movie later proceeds to include scenes in which Hanssen is interacting with others, and we overhear his thoughts. But unless one follows the movie very closely, and notices that his mouth is not moving, the voice-over is indistinguishable from conversation, so the result is confusion rather than greater understanding of his motivation.

Intellectually, the device of the mirror image has a great deal of appeal. The doubled image gives a sense of the split personality that seems the perfect representation of Hanssen, without having to work in a satisfactory device that both fits with the plot and is suitably visual for revealing the psychiatric diagnosis. The device of the mirror image also has significance in relation to Hanssen's role in the intelligence community. The title of the television documentary, and the book which accompanied it, is "Into the Mirror: the Case of Robert Hanssen." "Into the Mirror" is a reference to the description of intelligence as a "wilderness of mirrors." The "wilderness of mirrors" was a phrase coined by Angleton to convey the difficulty in counterintelligence of distinguishing friend from foe, the layers of deception and impossibility of ever being certain who to trust. Hanssen used the "wilderness of mirrors" as camouflage for his betrayal. The use of mirror-imagery, both in the movie and in other espionage references,

evokes another likely suggestion in the minds of most Americans: Lewis Carrol's *Through the Looking Glass*, where on the other side of the mirror is another world that seems both like and unlike our own. Hanssen enters "into the mirror" in the sense that the appearances of normal life go on, but the appearances are concealing rather than revealing and disguise the many ways in which he does not fit with what his various relevant communities consider normal. The world of espionage in general can be described in much the same way. It's *Alice in Wonderland* all over again, including both the humourous strangeness and the discomfiting alienness.

The division into a two-part show was inevitable, given the constraints of the television medium. The division has an interesting effect, in that the division of the first half from the second creates in the story an arbitrary and powerful punctuation that isn't part of the natural flow of events, and isn't reflected in other media accounts. The division allows the first half to focus entirely on representing Hanssen and his motivation, and the second half focuses almost entirely on the role of the FBI in catching him. The FBI didn't really deserve much credit for catching him, but the juxtaposition suggests just that. It implies a natural, inevitable sequence: those who choose to commit crimes will eventually be caught. This is precisely the message the FBI wants promulgated in the media, and indeed, the FBI had served as consultants working with the producer. The FBI has long been considered skilled at public relations, in the habit of working with the media to produce a vision of reality that is friendly to the law-enforcement agency.[52]

Newspaper Coverage as a Constraining Medium

The newspaper coverage of the case follows a different pattern than the largest part of the television coverage. The evening news format is more sharply constrained than any of the other channels considered here, and seldom involved more than a single sentence updating the status of the case accompanied by an image of Hanssen behind the anchorperson. The television movie coverage focused largely on the question of motivation, and partially on the mechanism by

which communication was achieved, in that the symbolism of the footbridge where Hanssen and the Russians both left packages served as a leitmotif that recurred at each pivotal point. The newspaper coverage, shaped by the constraints of print journalism, focused more intensely on establishing harms rather than emphasizing motivation as intensely[53]. Turning to the Ames case for contrast, significance could be established by emphasizing that he was the highest-paid spied ever, and instead of emphasizing only the harms, significance could be established as evidence of our own intelligence agencies' lack of intelligence and incompetence at catching a mole. Hanssen has no similar external proof to support the significance claim, except the small point that he is the first significant spy in the ranks of the FBI instead of the CIA or military.

The strategy for establishing harms in the Hanssen case relies almost exclusively on the power of silence, the same rhetorical strategy that was observed in the Lee case where it was used to support the lack of evidence that could be shared regarding China's military progress. In the Lee case silence was a useful strategy, but also a necessary one because the evidence in many cases did not exist, and in other cases existed but could not be shared without ruining ethos. In the Hanssen case the silence strategy is clearly a deliberate choice, a preferred alternative when compared to other available possibilities. Thus it is in some ways a clearer example of the power attributed to the strategy of increasing secrecy to support an argument rather than sharing evidence.

Consider the media coverage in the national newspapers around the May 2001 indictment of Hanssen on official espionage charges. At this point in the coverage, the government had recognized that a strategy of downplaying the case would not be possible, because Hanssen was going to fight the charges rather than plea-bargain at this time. A trial is necessarily a public, non-secret rhetorical forum. So in order to prosecute, the government had to make a series of decisions as to what formerly-secret information they were willing to use in the interest of punishing a spy. This was always viewed as a weakness when considering the Atomic Energy

Act, as pointed out in a 1948 Harvard Law Review of "Some Evidentiary Problems Posed by Atomic Energy Security Requirements." In the cases prosecuted by our intelligence agencies, and in particular our domestic intelligence agency, the presumption has to be that since the "enemy" already has the secrets, they should be used in the prosecution because it doesn't matter if the American People learn the erstwhile secret. The Justice Department had indeed reached the conclusion that they would use every document that had been sold to the Russians as supporting evidence to their case. Having made that decision, the government was seeking[54] increased publicity rather than downplaying the case. So the media had access to all the documents that were also used in writing the books about the case, and which detailed what documents were sold, even though not in each case the exact details within each document. So, for example, we know that one of the documents sold included plans to continue agency operation in case of government and budgetary shutdown, but we don't know precisely what those plans were.

Given the government's strategy, one might expect that the media will share this information as part of emphasizing the harms in the case, which in turn underscores the significance of each article's coverage. The glut of information is familiar from media coverage of most other crime cases, and sometimes results in criticisms about violations of victims' privacy. But instead, of the seven national newspaper articles that immediately addressed the indictment, only one shared any significant information about the harms. The other articles instead stated (sometimes repeatedly) that Hanssen had sold "technological secrets." Apparently, "technological secrets" are by themselves significant enough to establish harms. In fact, apparently the declaration of "technological secrets" carries more weight than the listing of specific documents sold (many of which cannot accurately be described as "technological" except in the broadest sense of that term as an externalized and formalized mechanism for doing something.)

The following quotes are representative of the newspaper coverage:

"Technical secrets disclosed by Hanssen" Washington Post, July 7, 2001

"Based on the indictment, former CIA director R. James Woolsey said that Hanssen appears to rank behind Ames in terms of 'the people he got killed.' But in terms of technical secrets, he may rank with, or ahead of, the Walkers [a family spy-ring selling naval codes and techniques]" Washington Post, May 17, 2001

"A plea bargain would allow intelligence officials to plunge more quickly into the laborious task of debriefing Hanssen and to figure out exactly what secrets he may have given the Russians." Los Angeles Times, May 10, 2001

"Presidents–on both sides–demand information on which to base their policy decisions, and secret information is highly prized. Intelligence obtained clandestinely has a special cachet." New York Times, March 25, 2001, an article by David Wise (author of several books critiquing intelligence agencies and several spy biographies)

In each of these examples, the secrets that Hanssen sold to the Russians are not identified. No evidence is provided that he has harmed the nation's security. Quite to the contrary, the question of *what* Hanssen did is glossed over with a silence that reiterates the fact that secrets were sold. The secrets are left as just that: secrets, and more particularly technological secrets. This is important particularly when we understand that alternatives were clearly available to the newspapers, as shown in the one article I found which chose to support the significance of Hanssen's harms to national security with evidence. It is taken from the Los Angeles Times, May 17, 2001:

> "... argue that Justice would be better served by a full debriefing that would reveal which secret programs were compromised.
>
> · In 1986, Hanssen told the Russians that the United States was 'exploiting' a technical weakness in Soviet satellites to intercept transmissions.

- Two years later, he helped the Soviets protect their communication by disclosing a limitation on what the National Security Agency could read.
- In 1989, he turned over a top-secret analysis of U.S. plans to ensure the continuity of government in the event of a Soviet military attack.'
- Hanssen betrayed six Soviet citizens and agents who secretly were working for the United States in addition to the three KGB double agents mentioned in earlier filings."

Notice that when listing the specific secrets, the one listed last, which is the position of greatest impact, brings us to a familiar topic. The betrayal of agents, and the implicit link to their deaths, is the preferred way to meet audience expectations regarding harms. The Times does not mention here that the agents betrayed were also betrayed by Aldrich Ames. The "earlier filings" referred to here are from the first coverage of the arrest, and at that time the existence of the tunnel under the Soviet Embassy was the only other secret publicly known to have been compromised. The existence of the tunnel is a revealing choice for the first "secret" to have been released to the public. A tunnel for eavesdropping is a popular device in spy novels, largely because it was a device used frequently during and shortly after World War II. The Russians themselves had done the same thing to our embassy in Moscow, which we discovered through the use of a spy satellite that used infrared sensors and was able to measure the change in ground temperature that the tunnel created. The Russians had used numerous other techniques to eavesdrop on the American embassy in Moscow over the years. A tiny microphone inside of the wood carving of the American seal that was given to the embassy on the occasion of its opening allowed the Russians to listen to everything said in the embassy's main room for twelve years before the microphone was discovered. When a new American embassy was constructed during the early 80s, the Russians planted numerous bugs in all of the walls, and created secret means of entrance by using hollow columns in place of solid columns

for some of the supports. A skilled agent could have climbed up through the columns and access any floor of the building chosen. So this tunnel under the Russian embassy "secret" cannot have been a great surprise to the Russians. Their protests when, upon Hanssen's arrest, the secret was made public to the American people, were pro-forma in the same way that our protests had been pro-forma during the 70s: neither indicated any intention to change diplomatic policy, or to significantly alter their intelligence practices. No actions accompanied the words issued by low-level officials regarding the espionage.

PRIOR DISCOURSE CONSTRAINS SUBSEQUENT DISCOURSE

The fact that it had not been known Hanssen had revealed this secret until his arrest suggests that the Russians did not change their behavior in any way that we could notice when they learned about the tunnel. U.S. intelligence did notice when we ceased being able to intercept their satellite messages, but that evidence could have been interpreted differently. The change could be indicative of the Russian scientists having figured out the weakness themselves, rather than the result of espionage. The intelligence community knew to be looking for a spy, and therefore interpreted the evidence to support the hypothesis of espionage, because during the debriefing of Ames after his plea-bargain, it became clear that secrets that he had not given away had been compromised. The precedent set by Ames encouraged both the CIA and the FBI to interpret ambiguous evidence in light of the possibility of another spy. The inability of either agency to locate that spy had two consequences: one, the leading suspect (not Hanssen) was sidelined into less vital intelligence work. He has since been compensated with back-pay for the raise that he otherwise would have presumably received, and promotion. The other consequence is that we knew to target very specifically what intelligence we wanted from the Russians, and which sources were most likely to be able to supply that intelligence. This targeted search was accompanied by the offer of seven million dollars for the desired information, with evidence to support it. Within three years, this targeted search produced the desired result. The Russian

defector brought the entire file that the Russians had on Hanssen, providing more evidence for this trial than in any other recent case.

The success of garnering specific, targeted information can be seen here in the Hanssen case, and can be seen in more recent intelligence work as well. This intelligence work departs from the usual procedures in the intelligence world. Purchasing secrets necessitates disseminating as widely as possible what information we are looking for, and that we are willing to pay for the information. The strategy relies on openness rather than secrecy regarding the goals of the agencies. The information garnered is usually kept secret only temporarily, until a suspect is apprehended. Once the suspect is being held, the information is not only not kept secret, it is trumpeted broadly to show the success of the agency. The only secret maintained in some cases is the name of the informant. The FBI in particular, and to some extent the CIA, uses protection of sources and methods as the most frequent reason for keeping secrets[55], representing 75% of FOIA exemptions claimed, but the secrecy can be justified on the basis of protecting personal privacy rather than as a threat to national security.

Narrative Conventions as Prior Discourse

The Hanssen story is further complicated as narrative because it does not fit neatly into the standard good-guy/bad-guy format. Hanssen is easy enough to cast as a villain, but identifying a hero is complicated. In espionage stories generally, the preference is to cast the investigator who leads the search as the hero. One of the books written about Hanssen, Spy Who Stayed out in the Cold by Adrian Havill, did exactly that, using the strategy that we saw used in relation to both Ames and Lee, of interspersing chapters focusing on the hunter (the investigation) and the quarry (the spy). The strategy is less effective in the Hanssen case because the heart of the investigation, or at least the part which was eventually successful, had nothing to do with the team officially appointed. The "hero" of the successful part of the investigation would have to be cast as the Russian, whose defection with files gave us the Russians' side of the story. An unnamed Russian

does not make a good hero for a spy novel. For one thing he is a spy himself, one who betrayed his country and sold the names of all his country's assets, all for money. Just as we saw in the Ames case, it seems that Russia's national security has not been greatly impacted by this instance of espionage. The same rhetoric which turns Ames into a super-villain constrains us not to praise the Russian. For another reason, it is awkward to tell a story with a hero who has no name.

Gender Conventions as Prior Discourse

The easier story to tell in the Hanssen case is a variation on a love-story. Every telling of the story–in the news media, in books, on television–has given a prominent role to the women in Hanssen's life. The two women provide a dramatic plot device. The women are opposites, and between the two of them exemplify the Madonna/whore syndrome. Bonnie Hanssen, the wife, played the Madonna. She was extremely religious, and brings Hanssen to the Church and to God. She is a full-time mother, staying at home to raise their six children. She was also opposed to sex for anything other than reproductive purposes. Bonnie was a virgin when the Hanssens married, and she never, by all accounts, was willing to engage in anything sexually risqué. Bonnie was a puritan when it came to such matters, as close to a virgin as a mother could be.

By contrast, Priscilla Galey was a stripper, though not literally a whore. She had also, at various other times in her life, been a drug addict and a mother. When Hanssen knew her she had moved to Washington D.C. to start a new life, without drugs and also leaving her daughter behind. Priscilla's striptease act was designed to appeal to the lunchtime crowd of business professionals. She would begin wearing a full three-piece business suit, so that as she stripped her audience could easily imagine some sexy coworker whom they encountered on the job.

The perversity of Hanssen is more easily illustrated through stories focusing on the women in his life than on his espionage. Hanssen's espionage is more dramatic–more titillating, more exciting–when the specific details are kept secret and classified. The story of how he was

caught is not very dramatic. But the story of how he interacts with these two women effectively suggests something about a twisted character.

Hanssen dealt with Bonnie by turning her into a sex-object without her knowledge and against what her preferences would have been had she known. The devout and repressed Madonna-figure of Bonnie gets sexually degraded by her husband. Hanssen wrote pornographic stories about her, in which she first begins as a naive exhibitionist and ends getting gang-banged. He posted these stories on the internet, where they can still be found on various websites that collect sex-stories dealing with fetishes. Another time Hanssen surprised his wife after a shower to take some nude pictures of her. After lying about having no film in the camera, he persuaded her to pose sexily as part of foreplay. Hanssen secretly developed the film and sent the pictures to his friend in the military, quite aware and willing for the pictures to be shown to others in the division. Hanssen also installed a hidden camera in his bedroom. The camera was connected to the computer in his office, and to the television and computer downstairs. The computers had internet access via modem, but we have no evidence that images from the camera were broadcast. However, the scenes were recorded, and the FBI retrieved the images while searching the house. Hanssen used this local-area network to enable his friend to watch him having sex with his wife. Hanssen would invite his friend to stay the night whenever he was in D.C., and would on those occasions apply pressure to Bonnie to have sex while his friend viewed it on the television downstairs. On one occasion Hanssen informed his friend Jack Hoschouer that Hanssen felt so close to him that he wanted Bonnie to bear Jack's child. Hoschouer assumed the idea would get dropped, but when he returned to Germany Hanssen e-mailed to tell him to purchase Rohypnol, which is available in the Netherlands without prescription. They planned to give Rohypnol, the date rape drug, to Bonnie and impregnate her while she was unconscious. This perverse plan did not get put into effect because Hoschouer did not make the purchase, but it serves to further illustrate a point about the character of Hanssen. The pure woman becomes a sexual fetish.

Readers may wonder how such intimate details of Hanssen's life become public knowledge. Some details, such as the stories and the camera setup, became public as part of the investigation. After learning from the Russian's files that Hanssen was the spy, a team was assigned to tail Hanssen, his communications were monitored, and as part of the trial proceedings became public. The source for the plan to impregnate Bonnie comes from Jack Hoschouer. Why did Hoschouer choose to reveal secrets that undoubtedly were considered a betrayal by his erstwhile friend? One reason is because he had agreed to turn state's witness for the trial. Hoschouer was vulnerable to an expensive trial himself because of Hanssen's espionage. The files had included Hoschouer's name specifically, as a potential target vulnerable to recruitment. Hanssen had given the Russians his friend's name and suggested as much to them. It was also far from clear that Hoschouer had not aided Hanssen's espionage, or potentially known of it. Hanssen's parting gift to Hoschouer had been a book, The Man Who Was Thursday by G.K. Chesterton, a spy novel with significant passages underlined. Further, Hoschouer had been the subject of at least one recruitment attempt that he had not reported, as military personnel are required to do. "I was too dumb to recognize it as a recruitment attempt," Hoschouer said in his defense. But once put on the defensive thus, there was pressure to turn state's witness, and betray his friend. Hoschouer could argue that it was not a betrayal, because his friend had apparently never been the man he thought he was.

Priscilla Galey the stripper would presumably have been a more logical target for Hanssen's sexual fantasies, if he had been searching for exhibitionist or voyeuristic opportunities. But by most accounts, Galey and Hanssen never had sex. Hanssen took her to Hong Kong with him, bought her a Mercedes, and paid for her dental work. She expressed willingness to have sex with him while they were in Hong Kong, but he insisted on paying for two separate rooms and did not even stay around to watch her bathe. He watched her striptease act frequently, but in the

more intimate one-on-one setting of traveling abroad together, he did not transgress her privacy even to the extent of seeing her nude, as he had numerous times on his lunch break in D.C. Hanssen's motive seemed to be trying to "save" Galey's soul. He pressured her to attend the Opus Dei church that he and his family attended, though she never got further than driving to the parking lot for church services. Galey was the beneficiary of the vast majority of Hanssen's espionage money. One possible explanation is that she was his "charity," to assuage his conscience. Had Galey been some other form of charity, the discourses about the Hanssen case would probably not have focused as much on the role of the charitable donations. Only one paragraph in any of the accounts reviewed, mass media or book or television, addresses Hanssen's donation to Mother Theresa's charity, when he was told by his priest during confession that he had to give the money from his first espionage attempt to charity and Bonnie helped select the charity. Contributions to the Priscilla Galey charity, if indeed that is how Hanssen viewed such contributions, receive much greater public attention. And Galey did receive a lot of attention. Consider a representative sample from the various books about Hanssen. Two out of sixteen chapters discuss Galey in Havill's book, two out of thirty-one chapters deal with Galey in Wise's book. Considering newspaper articles, there are only a handful (approximately 20 out of 336) which do not make some reference to the stripper. The storyline–eccentric rich man raises stripper to pedestal, treating her as a princess–sounds familiar, with echoes of Cinderella and Pretty Woman. The poetic and familiar storyline obscures the perversity of this roleplay. Perversity is meant to include not just turning something pure to an impure use, but turning that which is impure to a use for which it was never intended. The salvation of Galey is the flip side of the same personality that engendered the degradation of Bonnie. He reverses the roles of the two women in his life.

The coverage accorded the two women is striking for another reason. Neither one is integrally related to the story line about espionage. Bonnie would have to enter the story briefly

at least, because of her earlier discovery of his first espionage attempt. Her role is also important in that she controlled the finances, and thus served as a constraint. Her alertness contributed to the long stretches of time during which Hanssen did not communicate with the Russians, as did the FBI practice of requiring agents to serve in different locations throughout their careers. But as far as the espionage storyline is concerned, Bonnie's role is no larger than that of Hanssen's first two subordinates, Azbel and ???, who also grew suspicious of Hanssen and almost caught him, but who never receive more than a single paragraph of notice. Bonnie's ignorance was complete. The usual prosecution strategy of threatening to prosecute a loved one in order to force a spy to plea bargain was not even attempted because she was so isolated from Hanssen's activities. In most other espionage novels, which are after all part of the action-adventure genre, the wife does not play such a prominent role. Galey never knew anything of Hanssen's career, and could never have guessed at his espionage. It could be argued that her role is relevant to the story in that it shows Hanssen's duplicity. Hanssen was used to keeping secrets, in all aspects of his life.

There was a third woman who played a role in the Hanssen case worth considering. Kimberly Lichtenberg was Hanssen's first secretary when he was promoted to a supervisory position in the counterintelligence division at FBI headquarters. Lichtenberg was physically assaulted by Hanssen, and was awarded a large sum for worker's compensation in return for her silence. Hanssen had called Lichtenberg into his office at the end of a workday to attempt an interpersonal intervention, for he felt she was not getting along well with other administrative staff. She declared there was no problem and left to catch her carpool home. Hanssen ran after her, grabbed her and threw her against a wall shouting. He let her go when he realized there were witnesses watching, but had already done damage to her shoulder and neck. The violence of the largely-unprovoked assault should have sent some warning signal, but the warning seems to have gone unheeded.

So the role of the women in Hanssen's life is not related because of their integral importance to the story line. The women play such a prominent role in accounts of Hanssen's espionage for two reasons. One is that they stand in as an allegory, allowing the secrets to stand as enigmas rather than being explored. The women serve to prove that Hanssen was perverse and treacherous. The women also serve to satisfy audience expectations. The audience for an espionage discourse expects to find excitement, and Hanssen's actual espionage actions were not very exciting. He went on short walks in the park behind his home, where he both left and retrieved packages occasionally. The action is a far cry from the dramatic, shadowy meetings, evading the pursuit of a tail, and fake identities that we associate with espionage based on James Bond films. The story of Hanssen's women fits the stereotype much more closely. Additionally, the women are present in every account because the excitement of espionage and the excitement of sex are often correlated in the minds of modern American audiences.

Comparing Gender Roles Across Espionage Discourses

Every espionage case which we have considered here also incorporated women as part of the discourse in a related role. Intelligence work is a tremendously male-dominated field. This is hardly surprising, given that the CIA for so long drew much of their personnel from the military. Even today, the CIA hires fewer women than men and rarely sends women to be field agents, though they are able to rise through the ranks of analysts. The CIA has some good reasons for this apparent discrimination. Given that a good field agent needs to be able to blend in and operate smoothly undercover, and given that in so many of the regions where the CIA is most active tend to be areas where women's roles are more sharply curtailed than in the U.S., it is likely that women would not be able to function as effectively in the field. The FBI under Hoover did not allow any women to be field agents, partly because women could not fit with the "G-Men" image Hoover fostered and partly because field work was held to be too dangerous. Until 1971, the FBI employed women only in administrative positions (Insidious Foes, chp. 9).

There are, of course, exceptions to the marginality of women in intelligence work. Two of the most famous spy cases in recent history have involved women in a central role, but these exceptions prove the general rule about women's marginality. Even in stories where women play the role of the protagonist, the actual sources of the information are still always men. Consider, for example, the largely-fictionalized case of Mata Hari, which was originally based on historic accounts but gets embellished in popular recountings. Mata Hari is a name that today we associate with exotic seduction, with an element of danger. Historically, she was a Dutch actress of possibly Javanese descent during the time of World War I. After living in Java with her husband and losing her children, she moved to Paris to start a new life. She took a new name, began working as an "exotic dancer" (today we would call her a stripper), and attracted a large following, especially among the French military. When war broke out with Germany, she was recruited as a spy, but later was suspected of being a double-agent and executed. She herself served as a courier, but was not the originator of any intelligence, nor could she realistically be accounted a traitor, since her identity was not falsified beyond the use of her stage-name.

The second exception to the marginal role of women in espionage is the case of Elizabeth Bentley, the so-called "Red Queen." Bentley was the star witness at the vast majority of the early Red Scare trials. She testified against Whitaker Chambers, Alger Hiss, William Remington, and numerous others. As a witness she was rhetorically effective precisely because of her gender role, which she emphasized in court and in the media in a way distinctly counter to what we know of her interpersonal relationships (see "Elizabeth Bentley and Cold War Representation: Some Masks Not Dropped"). Bentley was caught by an FBI investigation of her lover, an illegal working for the Soviet Union. She was working as both a courier and the coordinator of a spy-ring centered in Washington D.C. and largely targeting State Department and other cabinet-level information. In trials, Bentley would frequently grow tearful, and would repent at length for her "wrongs committed in the name of love." By establishing her motive as one appropriate for a

female, she could safely reveal a vast knowledge of the operations of the Communist party and their intelligence collection without fear of reprisal. She could thus serve as a useful witness, even in cases where in retrospect it is not entirely clear that she had any knowledge upon which to base her testimony that so-and-so was a godless Communist spy.

In both of these cases, even though the female role becomes the central focus of the story, the women are not the source of information, but merely the channel. This marginalizing is inevitable, given that women in fact were not allowed legitimate access to secrets. Access to secrets is a form of power, which was historically largely off-limits, and women's role as the "weak" sex dictated against entrusting them with secrets.

We would expect to find that espionage stories the vast majority of the time would not include women in substantial roles, considering how marginal women's role in intelligence collection was. On the contrary, in fact we find that many espionage stories do include women, usually in one or more of a few set roles. Women can be agents of the enemy, working to seduce the protagonist. Women can be helpless victims. Women can be helpers, sometimes as tools useful for a mission and sometimes as a symbol of the good to which the protagonist must remain true. We recognize these stereotypical roles from Bond films and historical accounts. Even in those rare historical accounts that do not involve some role for women, such as the stories about Kim Philby and the Cambridge Five, there will be equivalent roles played by men.

In more recent espionage discourses, there still seems to be a compulsion to include women in some role. In the Lee case, for example, his wife Sophie plays an important role in demonstrating the purported duplicity of the Lees. Sophie gets cast in the role of the enemy agent. The fit is awkward in any telling of the story. Sophie was working for the FBI, not the enemy counterintelligence service, when she hosted Chinese visitors and maintained frequent contacts through letter-writing and helping them with library requests. But the elements are all there–contacts with foreign agents, duplicity of purpose, and a non-feminine assertiveness. The

story about Sophie's battles with her supervisor about the time she spent working for the FBI with Chinese visitors at LANL have no real relevance to Lee's espionage or lack thereof. Yet as part of the investigation, Sophie's insubordination[56] was evoked in the media and in later books as evidence of untrustworthiness. Lee's daughter Alberta also gets included as part of the narrative, when the emphasis on Lee's persecution and possible innocence. Alberta is cast in the role of the helper, and her statuesque good looks (she's unusually tall, particularly for a Chinese-American female, standing at 5'9" or so) represent visually the role she plays–upright, innocent, and properly feminine.

The Ames case also includes women, and again the roles associated as typical of the female gender shape the roles that the women play in later discourses about the case. The story could not be told without reference to each of the women. The roles of the women must be cast publicly in a way that makes sense in accordance with their gender. This requires some new inflections on the traditional roles, for the Ames case represents one of few cases where the women's roles drive the action of the story. One of the interesting aspects of the Ames case is the uses to which the narrative is adapted after Ames' incarceration. Initially after the arrest of Ames, the narrative was used to illustrate the incompetence of U.S. intelligence agencies. Roughly ten years later, the narrative is used as an illustration of successful counterintelligence, and re-told with Ames almost absent from the storyline. For example, at the International Spy Museum the video shown on the screen in the lobby represents the Ames case through the use of two of the women who led the investigation.

Rosario Ames, as the wife, would traditionally have been cast in the role of the helper, if Ames had been the protagonist of a stereotypical spy novel. Instead, Rosario becomes a villain, and to emphasize her villainy she is portrayed in a role that is decidedly not properly feminine. Rosario becomes known to us primarily through the channel of the bugs in her house and tapping of her phone during the final stage of the investigation. The transcripts of the conversations

overheard are only quoted sporadically, and in the quotes Rosario appears a harridan. She nagged, she made demands, she belittled her husband, she screamed and cussed. Rosario's demands for material goods are portrayed as a large part of her husband's desperation for money initially. It was Ames' marriage to Rosario that triggers his first espionage, because the debt with which he was saddled from his previous marriage left him feeling he would be unable to provide for her in the manner to which she was accustomed.

Diana Worthen was an administrative assistant and a friend of Ames before he married Rosario. Worthen's role fits well within traditional gender roles, which suggests that she must be cast on the side of "the good," and indeed she is. Worthen remained friends with the Ames', and because of her closeness was able to see the amount of money that they spent. She was also an assistant to the counterintelligence investigation initiated to find what had happened to the network of Soviet agents. Worthen thus knew about the investigation, and also knew about Ames' money, and eventually connected the two after realizing that Ames' money was turning him into somebody other than the friend she had once known. Worthen does not usually reappear in the stories told about Ames, because her role as both feminine and a traitor to her friend seems to create an uneasy juxtaposition. Worthen appears in the Hanssen case investigation as well. Again her role is a proper feminine role, this time as a peace-keeper attempting to reconcile opposing men, who represented agencies competing for control of the investigation. The FBI and the CIA struggled over control of what eventually became the Hanssen investigation, code-named GRAYDAY. The investigation had gone through numerous permutations between the time of Ames' arrest and Hanssen's arrest. During the debriefing of Ames, it became clear that Ames had not known all of the secrets that the Russians had learned. The most glaring example was the case of Felix Bloch. Bloch worked for the State Department, and had an expensive mistress to cater to his sadomasochistic urges. The FBI was attempting to build a prosecutable case against

Bloch[57], and had tapped his phone and had a team tailing him. The tapped phone revealed a conversation between Bloch and a Russian believed to be KGB, in which Bloch was warned that his friend was sick so they would be unable to meet, and that "it was believed to be contagious." The FBI interpreted this as a warning about their surveillance, and indeed their continued surveillance showed Bloch carefully avoiding even minor legal infractions–including his mistress. How did the Russians know about the investigation, if not for a mole? But Ames could not have known about the investigation–he was serving in Italy at the time, and the investigation was being conducted by a different agency .

After Hanssen's arrest, it became clear that indeed Hanssen had been the one to reveal the investigation, though he had nothing but contempt for Bloch, believing him to be stupid and immoral, "but then he was a friend of Yours [the KGB]," so Hanssen moved to protect him. The warning to Bloch was the telltale clue that Ames was not the only counterintelligence problem, and the FBI and CIA had numerous and competing hypotheses about what should be done next. The executive order signed by Clinton after the Ames case required that all mole investigations be conducted jointly by the CIA and FBI, with the FBI taking the lead role, but the CIA's representative was not used to ceding control. Worthen served as the peacemaker in the group, coordinating the various offshoot investigations, until she retired in 1999. Because of the relative unproductivity of the investigation group, however, her role was never mentioned in the mass media, and only once came up in any of the books.

By contrast, the team investigating Ames received tremendous press coverage, and almost every book written about Ames follows a pattern in which by the second half the investigation team gets equal or better billing with Ames himself. There were five members of the investigation team during the phase that focused on Ames, and the most highly-ranked member was Paul Redmond, who later became the analyst responsible for identifying security weaknesses at the Department of Energy in the wake of the Lee case. The key to cracking the case was the

tracking of finances, made possible by changes in banking laws passed in 1985. The team's accountant was Dan Payne, who received little credit for his role[58]. But the investigation team is usually portrayed as having been led by two women, Jean Vertefeuile and Sandy Grimes. Leading a counterintelligence investigation is not a traditional role for women, yet they were clearly on the side of "the good." Therefore rhetors reviewing the case must reconcile this seeming tension. This is generally done by emphasizing the motive behind the investigators, not as professionals fulfilling the duties of their employment, but as women involved emotionally.

Jean Vertefeuille was always referred to as "the librarian." Her training was the same as that of any other agent at the CIA, and reputedly she excelled at marksmanship. The "librarian" at an intelligence agency has exceptional access to secret materials, and so to simply label her as "the librarian" seems slightly misleading. It conjures up visions of a grandmotherly woman, and indeed, Vertefeuile was nearing retirement when the investigation began, and when it ended she was officially retired and serving as a consultant. "The librarian" suggests a woman who is bookish rather than worldly, and is likely to be physically frail but patient and tenacious, qualities that might help given the mess that well-used libraries tend to be. Those same characteristics are attributed as the motivation of Vertefeuille. Her tenaciousness in particular is remarked upon and commended during the Congressional review, which singled her out for praise as the only individual who held the investigation together and kept them productive over the ten-year period of false starts.

Sandy Grimes is one of very few female field agents in the CIA, and was one of the first to be in charge of an operation abroad, as the operational officer in charge of Africa. Sandy plays the maternal role. She devoted her energy to the investigation because she felt protective of the assets she had been responsible for. Her determination in the pursuit that lead to Ames is compared to that of a "mother tiger" in one instance (Sellout). The most common quotation that is attributed to Grimes is selected to show Grimes as sympathetic. In speaking about the loss of

an agent she had recruited while he was serving overseas in Africa, she said, "I felt sick. I felt responsible. I tried to tell myself that the decision [to maintain contact when he returned to Moscow] had been the right one at the time. But those rationalizations didn't quiet my conscience. I kept wondering, did I do something wrong? Is it my fault?" (Confessions, p. 191)

ROLE EXPECTATIONS AS EVIDENCE

The peculiarity of attributing Grimes' motive to cast her in a more feminine role can be seen more clearly if we contrast it explicitly to the characterizations of Mike Rochford, who led the investigation in the Hanssen case. Rochford is described as resembling "an Ivy League English professor" in one instance, in another instance as "grey-haired at 45, slightly heavyset and soft-spoken." Further descriptions of Rochford emphasize his similarity to Hanssen. The link between hunter and hunted is emphasized to add drama to the chase scenes. Rochford is also less frequently shown in photographs than Grimes when their respective cases are covered. Mike Rochford had initially been in charge of the joint FBI/CIA investigation that eventually led to Hanssen. Rochford was selected because he had tracked the KGB officer in charge at the Washington D.C. embassy, Victor Cherkashin, since 1980, almost twenty years. The belief was that Cherkashin was the individual most likely to know of any additional spies in the U.S. intelligence community, since he was the officer who had been placed in charge of the Ames case. Indeed, Cherkashin was also Hanssen's handler, so the connection was a valid one.

Rochford, an FBI agent, compiled a list of suspects who had access to all the "anomalies," the secrets that were believed to have been betrayed but were not available to Ames. The list contained well over a hundred suspects, mostly CIA agents. The investigation team led by Rochford carefully compared any sign of heightened activity at the Russian embassy, with activities of individuals on the suspect list. The Bloch case was the clearest of the anomalies, and so suspects whose activities correlated with the warning given to Bloch were the focus of the investigation. One of the key agents involved in the case, the man who had identified the KGB

illegal that served as Bloch's contact, was a CIA agent named Brian Kelley, and Kelley had access to several other secrets that appeared to have been compromised. The remaining secrets, which Kelley had not had access to, the investigators reasoned he might have learned by seducing female coworkers. Kelley is described as balding and not very outgoing, so it seems an odd stretch to conclude that he was seducing secrets out of agents who had sworn to protect those secrets. Perhaps the confidence in this hypothesis is further evidence of the pervasive linking between espionage and sex.

There was other evidence suggesting to the investigators that Kelley was a spy. He left the country and had frequent contacts with foreigners, and he had a map of a nearby park in his apartment with mysterious X's marked on it. There had been numerous observations of Russians in the area around the park. The investigators tapped Kelley's phones, and began tailing his every move. The tail had a difficult time keeping track of Kelley, and they strongly suspected that he was practicing evasive maneuvers to be able to escape, presumably to Moscow. They also observed two occasions on which he passed closely near a suspected Russian agent, and the investigation team hypothesized that information was exchanged this way by means of what is known in the tradecraft as a "brushpass." The longer surveillance was maintained the more suspicious behaviors were noted, but the suspected spy was too clever and skilled at tradecraft to be observed clearly doing something prosecutable. So the FBI arranged to try to trick him into fleeing, and thus providing evidence of his espionage. A stranger with a thick Russian accent called Kelley and warned him that the FBI had him under surveillance and provided an escape plan so that he could be smuggled out of the country. The next day Kelly reported the stranger's call to the FBI and the CIA.

Rochford and the investigation team were by this time sufficiently convinced of Kelley's guilt that they wanted him out of a position that entailed access to classified information, so they confronted him. For four hours they attempted to convince the accused spy to confess, in a scene

reminiscent of the tactics used to persuade Lee. The fact that espionage is punishable by the death penalty was mentioned more than once. Every member of Kelley's family was also taken in for questioning, and he was suspended without pay for a period of 21 months. After 19 months of this continuing suspicion, Hanssen was arrested. The "evidence" suggesting Kelley's guilt was shown to be nothing more than a series of coincidences. In spite of the paranoid reasoning inherent in espionage investigations, much of our everyday experience is made up largely of coincidences. The fact that Kelley went jogging in the park, and had marked the points at which he would stop and do pushups, is only a reason for suspicion for audiences expecting to find reasons for suspicion. The fact that the park where Kelley jogged was frequented by Russians is not a coincidence. It is a result of the fact that the FBI, the CIA, and the KGB haunt many of the same locales for business reasons and to keep an eye on each other. The fact that the park was also occasionally used by Hanssen for dead drops is a coincidence, but was not part of the "evidence" collected by Rochford's investigation.

The continuing offer of large sums of money to targeted KGB agents in return for any information about a U.S. mole was a separate investigation, headed by Neil Gallagher of the CIA. The teams were merged after Gallagher purchased the Hanssen file from the KGB, and connected it to the ongoing mole hunt to show Hanssen as the spy rather than Kelley. The fact that their Russian source was able to smuggle the original documentation out of Russia was an outstanding coup for the joint investigation team, and how they arranged this is still largely secret.

SECRECY'S ROLE

The case of Hanssen thus ends with as many secrets as at the beginning of the story. In "Know Thy Enemy: Changing Images of the Enemy in Popular Literature," Handberg points out that the protagonist in Western spy fiction is always an "essentially lonely male whose relationships are essentially manipulative in nature." (p.122) Handberg argues that with the end of the Cold War this kind of spy literature, which "reflects the concerns of society in a crude

way," has gone into decline. Given the parallels between fiction and fact in the maze-like world of intelligence agencies, the case of Hanssen suggests that it is too early to make such an argument. The morality of the spy's world may indeed become more ambiguous with the end of the bipolarity of the Cold War, as Handberg argues. The example of the Hanssen case could support such an argument. Hanssen remains an ambiguous, mysterious character because his motivation is largely incomprehensible. In our attempts to establish Hanssen's motivation, and hence come to understand his identity as a spy, the balance between comprehensible yet reprehensible cannot be found. Only by characterizing Hanssen's identity as sexual pervert rather than as spy are we able to create an identity that can sustain the role of villain adequately. The secrets he betrayed are left largely as mysteries, still secret by choice rather than by necessity. But the tensions inherent in secrecy, as both something that attracts and concerns the outsider not privy to the secrets as Bok points out, ensures that the drama of the spy novel will not end.

Wrapping Up Espionage Cases

From surveying the espionage cases in recent years, we can draw a number of conclusions that might be of use in considering the nature of espionage as a publicly interpreted crime. A comparison across cases might be useful for at least three reasons. We might learn something about the nature of intelligence work by drawing on the insights communication theory can provide as it was used as a lens for studying each of the three cases considered. We might also learn something about the nature of communication theory by testing it against three espionage cases. Finally, we should consider whether this comparison across espionage cases can suggest any conclusions that would be of broader use for society as a whole. These three areas will be addressed in turn.

CONCLUSIONS ABOUT ESPIONAGE FROM STUDYING COMMUNICATION

Dealing with espionage cannot be a mechanical matter. Espionage is about not just information, organizational structure, and communication patterns. Our success or failures in dealing with espionage have more to do with exceptions--in the intelligence organizations and among the public. Those expectations are created, rehearsed, and sustained by rhetoric, found in spy novels, movies, cold war history, and narrative conventions.

One commonality across not only these cases but across all espionage cases, is that successful prosecution relies almost always upon testimony as the dominant form of evidence. Ames' case required the testimony of the many who had observed his drinking, Hanssen's case relied almost exclusively on the written documents that were substituted for the spoken testimony of our source in the SVR (the KGB's successor agency). The Lee case would have hinged most heavily on the testimony of Lee himself for a successful prosecution. This reliance on the importance of testimony is not coincidental. Modern theories of communication provide a way of understanding why this necessarily should be the case. If symbolic activity depends most heavily

on the decoding (or "reading") of the receiver, then the most valuable if not the only way to *prove* that communication has occurred would be in those instances where we have the receiver's testimony. In the absence of the receiver's testimony, the reading strategies of those in the same community as the receiver will be the next best substitute. Hence the testimony of intelligence officials plays a crucial role for interpreting the "language games," to use Wittgenstein's term, of the accused for an outside audience of the judge and jury. Proving the sender's intention in espionage cases is every bit as problematic, if not impossible, as communication theory would suggest. Reconstructing the motives behind the sender's intention is an exercise that can appeal to ethos but not logos in any given case. This partially explains the importance of arguments concerning motive in every espionage case. The importance of understanding the receiver's community reinforces the talk about intelligence practices of an enemy country, as we saw in the Lee case and as Hanssen complained of in his communications with the Russians. Hanssen pointed out to his handlers, when refusing to meet outside of the country, that "it is a cardinal sign of a spy. You have made it that way because of your policy. Policies are constraints, constraints breed patterns. Patterns are noticed." The reliance on established practices prevents new intelligence practices and helps to prevent recognition of a successful spy. But the reliance on established practices is crucial to understand the reading strategies of the receivers of the coded information.

For another commonality across cases, notice that in each of the cases, the argument could be made that the organizations were suffering from systemic failure, and this is the proximate cause of the espionage. In two of the cases, had the rules that were written regarding the computer systems been enforced, the potential damage done by the espionage would have been reduced. Lee would not have been able to download the legacy codes, if the barrier between the two computer systems had not been breached with the assistance of the computer personnel. Hanssen would not have been able to sell as many secrets if he had not been able to get the

passwords of other users of the computer system. Password protection is part of the proper computer protocols that are supposed to be followed at any organization (the same rules are in place at Pitt, for example), but which were not being observed and are particularly crucial in an organization dedicated to secrecy. The systemic failures in Ames' case are more obvious, and were dealt with at length in the Congressional investigation: a culture in which excessive drinking was not counter-normative, in which negative evaluations were not shared, and in which the purported "enemy" was consorted with as peers.

There are other similarities beyond the organizational failures. All three cases present mid-level employees nearing the latter part of their careers. The spies were not low-level newcomers, they were individuals who had proven themselves in the past and shown loyalty by putting time into the organization. But all three were frustrated in their rise. Of course, what this commonality suggests for organizational practice in counterintelligence is difficult to put into effect: the individuals most in need of being watched are the ones set up to do the watching over others. This is clearly true in the case of Hanssen and Ames, who were both employed in counterintelligence and placed in charge of some segment of their branch. The role of watching is also critical in the case of Lee, in that his wife had been responsible for monitoring the behaviors of Chinese visitors to LANL. Ames suggested that something in the practice of intelligence, especially counterintelligence, tends to call forth the tendency towards treachery. If indeed counterintelligence responsibilities are corrupting, there is no way to fix this danger that appears across cases. The Webster Commission, investigating after the Hanssen case, recommended rotating employees through counterintelligence, so that nobody served for long periods of time. Counterintelligence works best by recognizing patterns over time, though, and a series of always-new personnel will be less likely to catch any relevant patterns.

The deeper questions raised for organizations by these cases of espionage include questions about who to trust, and what information should be controlled, and how this can best be done. The

lack of communication between intelligence agencies is acknowledged as a problem, and the decision to create a Homeland Security division of the executive branch of government is a reflection of this problem. The lack of communication is reflected in each of the espionage cases considered here: Lee, in the fact that the counter-arguments against prosecution were never forwarded to the FBI or Justice Department; Ames, in the fact that the FBI and the CIA search teams operated separately; Hanssen, in the fact that his brother-in-law's suspicions were not passed along. But as Tom Ridge, now in charge of coordinating domestic intelligence collection, has noted, in agencies whose primary mandate is secrecy and whose organizational histories have caused them to evolve into highly dissimilar cultures, an acknowledgment that secrecy between agencies is problematic is not enough to change material practices. The evidence that the secrecy creates problems is not sufficient to create the trust necessary in order to motivate secret-sharing, particularly not when secrets are the coin of the realm.

The problems with secrecy have been noted before as well. Every investigation into the practices of government secrecy has concluded that the best solution is to create fewer secrets and guard them more carefully. The Webster Commission in 1986, the Senate and House Intelligence Subcommittees after Ames, and Moynihan in his 1998 book all made the same basic point. And after every failure of an intelligence agency, the response is to try to reorganize the system. Most recently, that has meant creating the Department of Homeland Security, with the goal of eliminating the problems with inter-agency coordination. The goal is remarkably similar to that in 1947 creating the CIA. Then just as now, the failures of the intelligence system (to predict the Pearl Harbor attack, to predict the World Trade Center destruction) led to demand for reform and reorganization. Then just as now that reorganization took the form of a new agency, with coordinating responsibility. The Director of Central Intelligence is the title for the head of the CIA, but in practice he has never had much say over the practices of any of the numerous intelligence agencies other than his own, and 80% of intelligence money is actually under the

control of the DOD, which has little interaction with anyone other than the Pentagon and Joint Chiefs of Staff. There is no reason to believe that this is going to change with the appointment of a Director of Homeland Security to fulfill the same responsibilities the DCI was officially given when the CIA was created. There is no particular reason to believe that the additional personnel hired will improve our intelligence capability significantly, because simultaneously the responsibilities of the agencies have grown. While breadth of coverage may increase, it is unlikely that this will prevent future intelligence failures at a higher rate than our intelligence system has managed in the past. (Betts, 2002) The intelligence system that is so visibly under pressure to reform is the product of years of experience, with both failures and a significant number of real successes that shaped that system. The successes are harder to measure than the failures: how many spies did we prevent from sharing information? The answer can never be known, since it is counterfactual, and even if known would not be as public as the highly visible failures of intelligence. How many other terrorist attacks have been prevented? We know of only a few, as when we learned that the "shoe-bomber" Reid had been caught before boarding a plane, or when we learned of the arrest of two drivers attempting to suicide-bomb the Lincoln Tunnel in 1982. But how many more successes have there been that we do not know about, not because they are classified and kept as secrets, but because the plans were thwarted before they fully materialized–a chance encounter by a member of the group with a law enforcement or immigration officer that made proceeding seem too risky, or some other sign interpreted as evidence of imminent discovery?

The point is that reforms to the organization of intelligence systems are unlikely to make a tremendous difference. The systemic organizational failures are not failures of organization or bureaucratic structure, they are in some sense the result of having learned the lessons of past failures too well. Stringent measures applied to every aspect of an individual's daily work will

sooner or later cease to attract the notice and care that is needed for them to be effective, and this is an inevitable aspect of human behavior.

An increase in resources will also not likely solve the problem of potential future intelligence failures. Resources are less useful for "HUMINT" than for "SIGINT," because only if we happen to have cultivated a potential source do we even have the option of using said resources, and often money is not the best means for motivating a spy to work for us, or against us. The increasing feeling of alienation in the Arab-American community is likely to serve as a barrier that prevents intelligence agencies from effectively using additional resources even when those are available, as can be seen by the continuing difficulty the intelligence community is having trying to hire translators. For example, a recent article written by the Arab-American Association at the University of Minnesota included numerous quotes by individuals reporting their experiences being recruited by the CIA, and all reported refusing the offer. "I can't think of anybody who would be willing to serve in this capacity. They are in essence asking us to be informants. It would be too much like betrayal," Mareshe said. This is also a break from the CIA's traditional prohibition against domestic spying, altered since the passage of the Patriot Act.

Fixing counterintelligence is likely to be similarly problematic. Appointing watchers to watch the watchers becomes an exercise in futility. The question of "who do you trust?" cannot be practically answered by concluding "nobody." Counterintelligence in the new era, focusing on the war on terror, is also ever more obviously counter to civil liberties. The "secrets" we would want to protect include the location of our water sources, the sources of our energy, and the traditional information as well about our sources inside other organizations and our plans for handling contingencies. But the vast majority of this is information that citizens have a very legitimate need and right to know. We must know about our water sources, because it so often falls to citizens to protect those sources against pollution, and contingency plans today in many instances need to

involve citizens and individual-level preparedness. My claim is not that democracy is directly threatened by the increasing incursions on our civil liberties and the increasing secrecy of our government. Nevertheless, if we as a society grow more accepting of the claims for secrecy, the rhetoric of espionage and paranoia, then there are fewer opportunities for mistakes to get corrected, and it also increases the likelihood of future spies. The potential for a spy today, given the massive increase in secrecy, is much higher than at any previous time. Simultaneously, the damage that could be done by any single spy has in some sense decreased, in that we no longer have one single powerful enemy that we are continually at odds with, and that can compete as an equal in the battle to purchase secrets. Notice that in both of the most recent spy cases–Regan's attempted espionage and Anna Montes's espionage for Cuba–no money was contributed by any foreign government. And even aside from the question of whether a foreign government is able to access U.S. secrets, there is still a gap between that knowledge and any ability to take advantage of the knowledge to do significant harm. Greater integration of the intelligence agencies, if it ever happens, could increase the potential damage of a single spy. But more likely, the next "spy" is going to be an unwitting employee of some local feedstore being asked an innocent-seeming question and providing the key information, or a conspirator seeking employment at a potentially vulnerable agency and using whatever small bits of information become available in that capacity. The point is, counterintelligence against scenarios where the secrets are trivial and the opportunities plentiful, is almost impossible to be completely successful. This has been a trend becoming increasingly obvious even under the old Cold-War model of espionage–the increase in spies has not been coincidental. Others have made the same argument, such as Richard Betts in his 2002 article "Fixing Intelligence: The Limits of Prevention" in Foreign Affairs v. 81. The question is, what should be done about it? Betts' answer: don't bother trying. The secrets lost are not going to make or break national security. What will make or break national security is the

intelligence we collect, not what gets collected about us. Thus suggests that we need to be paying attention to the cultural conditions and discourse that give "meaning" to espionage.

A similar point could be made regarding what to do with counterintelligence failures when we do discover them. Prosecution does not seem to be a particularly effective option. Of the 105 espionage cases listed by the Defense Security Service, 42 cases, or 40%, ended in plea bargains. This percentage is perhaps more interesting when considered in the negative. That is, the cases not ending in plea bargains might be expected to end in the judge or jury finding in favor of either the prosecution or defense. But in fact many of those which did not end in plea bargains ended in non-judicial outcomes: a suspect committing suicide, or escaping to a foreign nation, dismissal of charges, or a declaration of mistrial. Those which ended in a court decision ended in a guilty verdict with only one single exception: the case of Henry Spade in 1988. The dynamic that resolves the majority of cases is that the government, in its role as prosecutors, has to date been significantly more interested in arranging to debrief the spies than in seeing them punished. The threat of the possibility of pursuing the death penalty gets used by the prosecutors to argue for a plea bargain in which the spy agrees to plead guilty to a greatly reduced crime or number of crimes and to cooperate with analysis of whatever damage was done. The dynamic can be seen in each of the cases considered here: Lee pleaded guilty to one count instead of 59 and was sentenced to time already served. Ames pleaded guilty to ten counts of conspiracy to commit espionage and income tax fraud. Hanssen pleaded guilty to fifteen counts of conspiracy to commit espionage rather than the 23 on which he was indicted. The dynamic becomes more striking still when a larger number of cases is considered.

The question of what to do with spies when they are discovered has been answered in a variety of ways other than the current dominant practice of arranging a plea bargain. During times of war, in fact, the U.S. seldom prosecutes a spy. Instead, the vast majority of spies are "turned," either by confronting them and persuading them to work on our behalf, or sometimes without their

knowledge. The spy is fed disinformation to pass to the enemy government. The lessons of World War II are striking in this regard. For example, Hitler had knowledge of where the D-Day invasion would land because he had an agent who successfully had access to the planning. He also had agents who were thought to have access, and who were deliberately given false evidence, even to the extent of creating faked-up models of fleets being constructed elsewhere, and deliberately sending our top general (Patton) to the wrong front. So given the plethora of contradictory information, the only possibility was to select which information to believe, and fortunately for us Hitler chose incorrectly. The disinformation strategy can be seen working against us today. The CIA and FBI had numerous clues regarding 9-11, but they also had a much larger number of clues that were false leads. The disinformation so outweighs the valuable intelligence, and sorting true from false is such a consuming problem, that in effect our intelligence system is unable to recognize the signal for all the noise. Using an erstwhile-spy for disinformation might be considered riskier than prosecution, since it removes the possibility of high-visibility prosecutions and hence might potentially eliminate a useful deterrent for others contemplating espionage. The question of whether massive penalties (including particularly the death penalty) do in fact function to deter others from committing crimes is an open question. But the main reason why spies are not more often "turned" is ideological. Recently General Brent Scowcraft declared that "the U.S. military does not lie," when he rejected the initiation of a branch of the DIA engaging in disinformation. The decision perhaps was in part motivated by publicity–the creation of the Office of Strategic Information Services had garnered concerned media coverage. The publicity upon creating a new office for disinformation does not explain, however, the consistent pattern of behavior, why the strategy of disinformation is almost never implemented. In an initial cost-benefit analysis of the merits of "turning" spies, spreading disinformation might seem the better policy. It's possible that such practices do get used, and that they are kept secret more successfully than any other aspect of intelligence work. Seems unlikely, though. Eventually a spy

would betray such a secret, and the American public would learn of the disinformation campaign, because the 1980 Supreme Court decision in *Richmond Newspapers v. Virginia,* 448 U.S. 555 declared that non-public trials violated the Sixth Amendment.

The prosecution of spies is almost never successful unless they agree to a plea-bargain. The publicity of trials guarantees that the government must choose to give up certain secrets to even attempt prosecution. The fact that they regularly choose to do so is perhaps an argument in favor of the earlier argument that less information should be classified. Significant resources must be dedicated to counterintelligence if even one spy is to be caught using means other than waiting for another to betray the traitor, which is still how the majority of cases get discovered. Surveillance is expensive, in terms of manpower and money, and the odds of targeting the correct suspect are low considering the ratio of spies to loyal intelligence community members. Consider some of the examples of the high costs: during six of the years of the Hanssen investigation, the FBI dedicated a team of twelve agents to tailing a CIA agent suspected of espionage, and dedicated another eight agents to investigating finances, travel, intelligence work, and other aspects of the case. In salary costs alone, as well as time, the costs are high, and this is not counting the cost to the individual suspected who was denied promotions or desirable work assignments. The investigation following a suspected North Korean spy (Yai) consumed nine years and 1.2 billion in costs.

The questionable value of prosecuting spies is recognized by the U.S. government in other ways as well. Spies are often put in prison only until they can be traded to another government in return for various favors. Often suspected spies are merely transferred to less-sensitive work. And for a period of ten years, the government did not prosecute a single espionage case. Between 1965 and 1975, not one spy accusation was brought by the government. There might be multiple possible explanations for this. One possibility is that considered previously in the Ames chapter: the government did not "choose" not to prosecute, but was instead unable to effectively prosecute

any espionage cases because of the disarray in counterintelligence under Angleton. Another reason why the government might have been unable to prosecute any cases is that the FBI at this time, under Hoover, was prone to using surveillance techniques that were not strictly legal and could not be admitted as evidence in a court case. There is another possible explanation for why no espionage cases were prosecuted during this ten-year period: perhaps the government was experimenting with other strategies for dealing with spies, such as using spies for disinformation, or perhaps putting them to use as analysts diagnosing flaws in the intelligence system. Even today, the intelligence agencies have recognized that using spies to improve intelligence work is more valuable than simply punishing them. The deterrence effect, if there is any, is less valuable than the potential insights gained from the spies themselves, particularly those clever enough to have been successful spies. Ames, for example, has been serving as a consultant for the CIA even after his initial debriefings, and his insights have been constructive. For example, Ames' cooperation enabled the FBI to continue mole-hunting, the search that led eventually to the discovery of Hanssen, and two other lesser spies.

CONCLUSIONS ABOUT COMMUNICATION THEORY FROM ESPIONAGE

The impact of espionage, or rather the rhetoric surrounding espionage cases, might be expected to have particular impacts. Frequent espionage cases encourage paranoia. Espionage encourages questioning the links between observed material conditions and history in favor of looking for links between material conditions and textual practices such as government intelligence policy and fictional forms. Espionage cases encourage audiences to accept a rhetoric of secrecy, which in turn necessitates trust in the rhetoric of authority. At the same time espionage rhetoric encourages distrust of other nations and of other individuals within our own nation. It tends to reinforce ties to nation-states, invigorating patriotism by constructing an unseen threat from both within and without and demanding trust in authority.

Hans Kung argues that we can seek ever more information, but no information ever will, nor ever can, bring us to a point of closure regarding the question of whether or not God exists. In the end, there must always be what he calls "the leap of faith." And it will always, inevitably, be a blind leap. It the leap is not blind, it is not faith. Some such faith seems to be required in understanding others.

We dream (have always dreamed, and I believe will always dream) of communication so pure (noise-free, the social-scientists whisper) that it can provide perfect information. John Durham Peters has pointed to some of the problems with this dream of communication. This dream for communication privileges dyadic communication, it privileges similarity over difference, and it locks us to notions of intentionality. Pragmatically there is another problem, because such "perfect" communication cannot happen. The more information we insist on collecting regarding one another, the more it obscures and postpones the inevitable. By forcing the other to try to convey meaning so clearly that we grasp it completely, we limit the communication to knowledge that in some way we already share. More information, more precision of meaning, can never answer for us the question of what exactly the person means, intends, or is motivated by. There must be a leap of faith, a decision at some point to either trust or not to trust that other human being. Information by itself cannot make that leap any easier. Information by itself cannot do anything until we fit it into our interpretive framework. The framework that we create individually, and the framework that we create as a community, is the bridge that we construct to try to shorten that leap, but it is our own, human and therefore necessarily flawed, construction. Rhetoric brings us to a predisposition to trust or not.

The best thing for both individual human relationships and for relations between nations (or other groups as we move into our "global village" era) is to make the leap of faith, to make the decision to trust one another. The decision to trust, even in the absence of information that fully justifies the decision, enables us to move forward, to form communities, which will in turn allow

in the future more perfect communication and eventually will provide justification for the leap of faith. Trust is the opposite of evidence. Communication that purports to play the role of evidence is ambiguous. In studying rhetoric of science and sociology of knowledge, scholars have returned time and again, from Hume to the present, to the realization that data (evidence) is always underdetermined. Facts do not stand alone, they have meaning only when we relate them to a system of other meanings. When we have communication that relates in a way that reinforces current systems of meaning, it can be counted as evidence. When communication clashes with the system of meaning, either it is not given status as evidence, or the system of meaning is forced to shift in relation to the new communication. That shift is the ending of trust.

Consider in relation to this the proceedings in each of the espionage cases we've looked at previously. In Ames' case, trust prevented the available evidence from being seen as evidence. It was not evidence until trust had been ended. The first breach of trust depended upon changes in the relationship between Ames and his friend Diana Worthen, who also happened to be involved in the search for a mole. But while trust persisted, even Diana, who had every bit of evidence available in the investigation all present in her head, still she could not see simultaneously both Ames who she trusted and the mound of evidence, not in relation to each other. But when Ames began treating her differently and more distantly, the trust was damaged. And then within a week she brought her suspicions to others involved in the investigation, and trust ended utterly. After this point, even had the evidence not supported suspicions of Ames, the trust could not ever have returned. Or consider the example of Lee. The evidence does not support the charge of espionage, but this does not restore trust. Lee is not guilty, but neither will he again be trusted enough to work at the lab, or relate as easily among those who did not already know him. Trust established previously among those who knew him beforehand ensured that the events mentioned by prosecutors would not stand in relationship to Lee as evidence, regardless, within their minds. Instead, the communication mustering such evidence is counted as evidence of the prosecutors'

racism. The case of Hanssen is harder to demonstrate the relationship between evidence and trust. In part this is because there was no evidence in Hanssen's case until the unnamed Russian's defection, so it could not be mustered regardless. But Hanssen was never precisely trusted, either. He was given promotions based on evidence that he knew more about technology and about the Russians than others knew, but he formed no relationships with those he worked among. The FBI did not have the same training or experiences in the field that created strong bonds of trust the way the CIA did. Hanssen remained an outsider referred to as "the Mortician" and "Dr. Doom."

Perceiving trust as the opposite of evidence is a counterintuitive conclusion for those approaching the study of espionage from a rhetorical theory perspective. Traditionally in rhetorical theory evidence should increase trust. The roots of this belief can be traced clearly at least as far back as Aristotle. Aristotle's famous definition of rhetoric tells us that "rhetoric is the ability to see in each particular case the available means of persuasion." Those means of persuasion are ethos, pathos, and logos. The word used in the definition is "pithanon," or persuasion. But the Greek term used elsewhere to refer to ethos, pathos and logos, which we usually refer to as the "modes of proof," the word for these three is "pisteis." And "pisteis" is usually properly translated into English as "trust." Aristotle's definition is in other words telling us that rhetoric is the art of creating trusts, which in English the majority of translations of Aristotle have turned into "proofs." The original insight gets lost. Does this difference in translation make a difference? I would argue that it does. In situations in which there is trust, no proof is called for, and to offer proof without call is as likely to diminish trust. There is a sense of "the lady doth protest too much," a suspicion that is created by proofs offered apropos of nothing. Even in situations where proofs are called for, because of a lack of trust, still proofs do not create trust. An accused criminal is never able to prove his/her innocence, only to deflect a particular accusation. Trust does not get restored. The same dynamic occurs in more everyday instances when proof is demanded as well–relationships where fidelity is questioned, a teacher raising

questions of plagiarism. Proofs cannot in fact create trust, because by definition trust is a leap of faith, a decision to interpret uncertainty in favor of the individual. So our translation of Aristotle's theory as creating proofs instead of creating trust gives rise to a couple of millenia overemphasizing the role of logos, and misunderstanding the basic goals of rhetoric in a way that complicates its relationship to philosophy and undermines its relationship to theology.

The etymology is instructive. The English word we use for "trust" derives exclusively from the German, and is of course the same root that we use to develop "true" and "troth." The Greek word "pisteis" does not enter into the English language in any form that is currently active, and also has no cognates in Latin, though Latin has 34 words[59] that can be roughly translated as "trust," including the familiar set of words based on "credo." The similarity between faith and trust, between trust in God and faith in our fellow humans, is emphasized in the Latin language. But we lose sight of that relationship in English. And we lose sight of the relationship between trust and persuasion in English, particularly problematic for the rhetorician relying on translations of Aristotle. The English word that we use instead of "trust," the word "prove," has a very different meaning than "trust." Persuasion is about establishing trust.

Yet Aristotle lists under his heading for pisteis the use of logos, and each mode of proof has both extrinsic and intrinsic versions. Extrinsic (or inartistic) logos, as has been explored more thoroughly by later theorists, includes the use of testimony and evidence. So following traditional rhetorical theory, evidence has long been treated as subsidiary to trust, as one of several possible means for creating "proof," which is treated as equivalent to trust. But what we see in these espionage cases is that extrinsic logos, or evidence, does not lead to trust. In fact, seeing evidence seems to undermine trust. Similarly, in public discourses related to espionage, trust in the current system is preserved by careful avoidance of evidence. The institutions that are most likely to challenge the status quo–those whose interests include representing a larger population of minorities, for example as with the Los Angeles Times –are the papers most likely to present

evidence in relation to an espionage case. Notice that in both of the cases where media coverage was studied explicitly, the Los Angeles Times was the newspaper whose reportage was least sympathetic to the government position. [need to check into Ames coverage]

What does create trust, then, if not evidence? Trust is the decision to take a leap of faith in relation to another human. The leap of faith takes the form of interpreting communication, which is always potentially multivocal, in the most favorable meaning possible. If trust is present, then behaviors which allow for interdependence can ensue. The surest route to increasing the likelihood of that leap of faith is the satisfaction of expectations. Expectations shape much of our perception. We are likely to only perceive something as evidence if it fits within our frame of expectations. Similarly, if an individual, organization, or event, fits well with our expectations, we are more likely to trust–in other words, to be persuaded by it.

For rhetoricians the significance of expectations has been noted many times before. Aristotle pointed out the crucial role of enthymemes in persuasion, which is to say that he highlights the importance of drawing on audience expectations. In more recent times every major rhetorical theorist has noted the importance of adapting to audience expectations. My point here is not simply that expectations shape the persuasiveness of a given message. The point is that evidence, in the traditional logical argumentation sense of the word, has no impact whatsoever on effecting persuasion.

Instead, persuasion should be conceived as a process of satisfying expectations. Our expectations come from a wide variety of different sources, and are not internally coherent or consistent. As we have seen in the case studies here, expectations can be based upon narrative reasoning, and the familiarity of stock characters and story types ("phenotypes" in the language of narrative theorists following Vladimir Propp). Familiarity is promulgated through shared discourse channels that circulate broadly, channels such as newspaper and television accounts, and importantly through books, both fiction and non-fiction. Our expectations can also come from

history. History in this case functions in much the same way that other narratives function. Unlike other narrative forms, the expectations established by history not likely to be as widely shared and familiar. The power of the expectations set up by history resides in their greater credibility. A third source of expectations that functions persuasively is based upon our understanding of human psychology. We have expectations based upon the roles that we see individuals playing, both in our own lives and in the wider world through various discourse channels. Our beliefs about motivation arise from these same sets of experiences. Expectations come from these varied sources, and are not consistent across them, or across individuals.

Achieving persuasion happens when a new set of expectations are invoked. The new framework of expectations then shapes responses appropriately, and those responses will be shared to the extent that the newly-made-relevant expectations are shared. Evidence in the traditional sense cannot accomplish this kind of gestalt shift by itself. At best it can serve as a flourish to ornament and accent an account that suggests a new framework of expectations.

In other words, here's how rhetoric works, at least in the context of espionage and intelligence work, which I think is an important microcosm of how it functions more generally. Trust is the deciding factor in determining what any individual will do. Trust occurs in an iterative cycle. The decision gets made to trust, which then allows certain interpretations of meaning and because of that certain possibilities for interaction and interdependence. Trust gets reinforced when expectations are satisfied, whether those expectations are positive or negative (i.e., that individual is likely to keep his word, or that individual is likely to try to take advantage of me). When new expectations are aroused as being relevant to a situation, an new definition of the relationship ensues. Different decisions about meanings will follow after that, and hence decisions about actions will probably follow.

CONCLUSIONS RELATED TO BROADER SOCIETAL QUESTIONS

Espionage rhetoric raises one third major area of questions. What is the impact of espionage on society? The central two questions addressed in espionage rhetoric are those of secrecy, and of betrayal. Secrecy has long been held as abhorrent to Communication scholars. Is secrecy justified in these cases? Is espionage a sufficient contribution to national security to make it worth the exception to First Amendment protection that it represents? There are moral objections not just to the secrecy, but to the lies that protecting secrets inevitably entails. The protection of secrets also creates a potential for corruption, and a form of power that is particularly inviting to abuse.

The secrecy invoked in espionage cases fulfills an important persuasive function. In each of the cases considered here, we see that the discourse functions be drawing attention to the secrets, to the discursive absences that are taking the place of evidence. This primacy of secrecy invites particular reading strategies. Those reading strategies are not the best ones for a democracy, as they encourage paranoia and a blind reliance on authority. The other potential harm of espionage rhetoric is that it undermines the First Amendment, in a way that cuts off the opportunity to question this exception without being labeled unpatriotic.

Espionage represents an exception to the First Amendment, and is one of the only forms of speech that is not only not protected, it is prosecuted, sometimes to the point of death. Espionage is communication made into a crime. Not necessarily just speech, but communication or any use of codes. Of course, espionage is not the only instance where speech becomes a crime, since particular types of threats or solicitations can also be crimes. But this form of speech crime is a particularly interesting violation of free speech, since it is also simultaneously a type of political speech. We can dismiss this as a negligible violation of the First Amendment, because after all when individuals go through the process of getting a security clearance, they know full well that they are voluntarily surrendering their rights to free speech on topics related to their employment. But maybe we should not be so ready to dismiss this exception to First Amendment protection,

because this exception undercuts the majority of the arguments offered and used historically supporting the First Amendment.

Most arguments in support of the First Amendment justify it on the basis of a consequentialist approach. The "marketplace of ideas" metaphor is the most frequent explanation for why communication of all sorts needs to be protected. This explanation is dominant in science as well, in which truth emerges from the clash of ideas so long as no artificial barriers are imposed. This is the argument that most often comes up in court cases, as for example Judge Learned Hand's famous use of the phrase in *U.S. vs. Associated Press* (1943). This same argument gets refined in the reasoning of Posner by drawing on economics models of the market to establish why many decisions that have allowed exceptions to the First Amendment are wrong. The "marketplace of ideas" depends for its functioning upon the lack of artificial restraints. Government secrecy due to espionage limits that functioning.. The "marketplace of ideas" can be challenged on pragmatic grounds, for there is no empirical evidence that such a free market is ever possible, or even if possible that it would function effectively. But a democracy does depend on the perception of some equivalent to a "marketplace of ideas," or at least justifying the free speech clause of the constitution seems to require it. The need for checks and balances in a democracy can only be served by a public that is informed about everything relevant for guiding their elected representatives. This "checking function" is also one of the most important justifications for the First Amendment, and serves as the basis of journalism's claim to be the "Fourth Estate," which has served as the grounds of many First Amendment decisions. This "checking function" is undermined by the secrecy surrounding espionage cases.

A third argument in favor of the First Amendment is based upon Rousseau's concept of a Social Contract, arguing that humans do not and perhaps cannot contract away their rights to freedom of expression, because the right of expression is so fundamental to the essential nature of humans qua humans. Support for this idea that expression is one of if not the distinguishing

feature of what makes us human can be traced back in the field of rhetoric to its very roots. This emphasis on expression as a distinctively human trait has also shaped the entire Western understanding of education, at least as far back as Isocrates. Isocrates argues that just as speech is one of the things that sets us above animals, so eloquence in speaking and analysis when listening are the mark of civilization as opposed to barbarianism. Numerous variations on this theme can be found in current First Amendment theory, including the social constructionist interpretations of the law, the law-as-literature approach represented by Stanley Fish, so forth and so on. And this argument is the one that gets most badly damaged by the growth of secrecy and increasing role of intelligence agencies if we believe that growth of secrecy spreads as a social construction. We accept the limitation on freedom of expression for those who accept employment in intelligence because it is taken on voluntarily. But what if communication is part of what makes us human? Can we really legitimately give up our right to communicate any more than we can give up our right to think? There are other situations in which we give up our right to speech on specific topics, as when we make a promise not to divulge a surprise birthday party, or to share a friend's embarrassing story. Usually in these situations the secret is temporary, and in other cases the promise is understood to be less-than-absolute. For example, no friend would be surprised if you told the investigating police about her secret affair after she vanishes, and would probably not be surprised if you told your own spouse.

The "marketplace of ideas" could most readily accommodate the need to create an exception to free speech for espionage. The argument is straightforward: the costs of the secrets and whatever distortion to the free market they create are counterbalanced by the costs that the damage to national security would be wrought by their revelation. To make this argument would require being able to quantify what the costs are to the marketplace, which cannot be done since the market does not function perfectly and has no demonstrable effect. But the argument would also require that we quantify the damage done to national security by espionage. And this cannot

be done either. Not only can the damage done to national security not be quantified, it cannot even be identified. The threat to national security presumably must mean that the secret could potentially alter the balance of power, could change the position of the nation that loses the secret. The point of counter-intelligence is to attempt to preserve the nation's security by preventing other nations from gaining information that could be advantageous enough to threaten our security. In contrast to the purpose of intelligence collection generally, which is to enable us to have knowledge on which to base our decisions, the point of counterintelligence is to prevent other nations from having knowledge that they might use in deciding their own courses of action. This might make sense if we are at open war, and the other country is a declared enemy whose decisions would necessarily involve attempts to harm us. The protection of secrets outside of wartime and the protection of secrets that are not directly related to troop-movements are less clearly relevant to national security. For example, allowing knowledge of the capabilities of our weapons seems to be largely advantageous, more likely to persuade another nation *not* to attack us than any harm.

The harms to national security by the examples of espionage considered here have demonstrably not been enough to alter the balance of international power. Hanssen's secrets did not alter the behavior of the Soviets, or change their relationship to the U.S.. Ames' secrets, which led to the deaths of our agents, were clearly damaging, but not clearly threats to national security. As a nation, our position of power was not changed, though he would need to be prosecuted regardless of whether it is treason, for at a minimum he was guilty of aiding in multiple murders. In principle, that change is the justification for why espionage is punishable by the death penalty, because of the risk the nation as a whole is placed under. But is that risk real, or is it merely a hypothetical possibility? I think you'll have difficulty thinking of a real espionage case in which national security was genuinely altered.

There are reasons other than damage to national security for labeling espionage criminal, and possibly for invoking the death penalty. The crime attaches the emotional attention that we see routinely expressed in the high publicity, because espionage is the practically the only form of treason recognized in the U.S. today. There have been strikingly few treason convictions in U.S. history. A survey of all the treason cases reveals that the vast majority of those which have been brought, have been overturned. So the full burden of communal outrage over treason falls on espionage cases. Treason is an important concept for maintaining a concept of community, and espionage represents a case in which the spy clearly demonstrated a lack of loyalty. Even though no harm came to the nation, espionage is a declaration that the individual lacks loyalty, in a way that can be punished and still be consistent with American ideals about the value of dissent and the need for diverse perspectives. For example, an ongoing case in Los Angeles today involves a U.S. citizen (John Yai) of South Korean descent, who has been sending information to North Korea in return for several thousands of dollars. The Koreans have been purchasing from him information that is not classified, primarily political information covered in the Los Angeles Times newspaper. Is this an example of espionage? It seems a betrayal, for the man is selling information to a country that particularly now is considered an enemy. But it is not clear that he can be charged with any crime beyond that of tax evasion. The First Amendment is rarely seen as an issue in espionage cases because at the heart of the issue, it matters little that the only thing that actually happened was that symbols (words, codes, in exchange for money, the symbol par excellence) were communicated. The criminality of it, the reason why the death penalty gets invoked, the unconcern over citizens' rights; all of this is because the spy has pretended to be an insider, and we believed, and the spy was all along an outsider by virtue of having no loyalty to the group. The betrayal of trust is what is at issue.

But the fact that a spy betrayed us does not, in fact, prove that espionage is a grave harm to national security. In the first place, we have not yet established that the information should have

been kept as a secret. In the case of the Pentagon Papers, Ellsberg and Russo were indicted on espionage charges, but in retrospect most people would agree that it is better that we the public understand what went wrong in Vietnam. We also have not yet established that the government, when it gets caught playing intelligence games that are the exact equivalent of the betrayal we are so outraged by, has a right to react by invoking the death penalty. Exile actually seems more like justice for such a case. Treason that has resulted in no material harm to the nation suggests that perhaps this individual who has declared a lack of loyalty should not be counted as an insider, and should be sent elsewhere in the exact same way that we deport foreigners found to be intelligence agents for their own governments. But since exile is forbidden by the constitution, we are left with life imprisonment or the death penalty for responses to espionage.

TOWARDS FUTURE RESEARCH

In her book Secrets, following her earlier study of Lying, Sisella Bok surveyed many of the common forms in which we experience secrecy. Unlike lying, she did not begin with a presumption that secrecy is negative, but in each chapter in which secrecy is combined with power, it needs strong safeguards if it is not to become negative. She stated, "secrecy can diminish the sense of personal responsibility for joint decisions and facilitate all forms of skewed or careless judgment, including that exhibited in taking needless risks. It offers participants a shield against outside criticism, and can obscure the possibilities of failure–especially if the decision-makers come to think that the situation resembles a game." Though she does not refer to intelligence agencies explicitly, the intelligence agencies fit her description.

Espionage is a violation of secrecy, and particularly of the type of secrecy that Bok is particularly thorough in condemning. Of course, this does not exonerate espionage in terms of ethics. But it does point to the difficulty of evaluating espionage. In terms of ethics and in terms of its effects, espionage is so shrouded in secrecy, and so lost in the wilderness of mirrors that is the world of intelligence, that evaluation is difficult. All of the public discourses regarding

espionage could well be fundamentally flawed, either deliberately misled or unintentionally but unavoidably riddled with errors and misunderstandings and omissions. The nature of espionage as a crime requires that we as readers also suspect manipulation. The public discourses we have considered here have included numerous texts from numerous sources, but the texts are notably interdependent, and that interdependence gives rise to the possibility that the similarities are strategic and intentional. Even aside from the possibility of national security interests dictating deliberate manipulation, it is clear that much is left out and remains secret. The layers of secrecy which remain could totally alter the tentative conclusions that might be drawn from this study of public discourses.

Perhaps the best note on which to conclude is the motto of the International Spy Museum: "All is not what it seems."

Bibliography

Adams, James. Sellout: Aldrich Ames and the Corruption of the CIA. Penguin Books, New York. 1995.

Barnouw, Erik. The Sponsor: Notes on a Modern Potentate. Oxford University Press, 1978.

Bazan, Elizabeth. "Espionage and the Death Penalty." Federal Bar News and Journal, v. 41-9, pp. 615-619. October 1994.

Ben-Yahuda, Nachman. Betrayals and Treason: Violations of Trust and Loyalty. Crime and Society series, Westview Press, 2001.

Betts, Richard. "Fixing Intelligence." Foreign Affairs, v. 81, pp. 43- 59. January 2002.

Black, Edwin. Rhetorical Questions: Studies of Public Discourse. University of Chicago press, 1992.

Blitzer, Wolf. Territory of Lies: The Exclusive Story of Jonathon Jay Pollard, the American Who Spied on His Country for Israel and How He Was Betrayed. Harper & Row Publishers, New York. 1989.

Blum, Richard, editor. Surveillance and Espionage in a Free Society: A Report by the Planning Group on Intelligence and Security to the Policy Council of the Democratic National Committee. Praeger Publishers, New York. 1973.

Bok, Sissila. Secrets: On the Ethics of Concealment and Revelation. Random House, New York. 1989.

Booth, Wayne. The Rhetoric of Fiction. University of Chicago Press. 1961.

Bourdieu, Pierre (transl. Priscilla Ferguson). On Television. New Press, New York, 1998.

Brummett, Barry. "Towards a Theory of Silence as a Political Strategy." The Quarterly Journal of Speech, v. 66, pp. 289-303. 1980.

Bunker, Matthew. Critiquing Free Speech: First Amendment Theory and the Challenge of Interdisciplinarity. Lawrence Erlbaum Associates, New Jersey, 2001.

Burke, Kenneth. Permanence and Change: An Anatomy of Purpose. New Republic Press, New York. 1935.

Burke, Kenneth. A Grammar of Motives. Prentice Hall, New York. 1945.

Canaday, John. The Nuclear Muse: Literature, Physics, and the First Atomic Bombs. University of Wisconsin Press, Madison. 2000

Cawelti, John & Rosenberg, Bruce. The Spy Story. University of Chicago Press, 1987.

Ciani, Maria Grazia, ed. The Regions of Silence: Studies on the Difficulty of Communicating. London Studies in Classical Philology, v. 17. J.C. Gieben, Amsterdam. 1987.

Cliffe, Lionel; Maureen Ramsay and Dave Bartlett. The Politics of Lying: Implications for Democracy. St. Martin's Press, New York. 2000.

Committee on Armed Services, House of Representatives. Results of the Department of Energy's Inspector General Inquiries into Specific Aspects of the Espionage Investigation at the Los Alamos National Laboratory. U.S. Government Printing Office, November 1999.

Committee on Science, Space and Technology, U.S. House of Representatives. Science Policy Task Force Report: The Regulatory Environment for Scientific Research. US Government Printing Office, Washington D.C.. 1990.

Earley, Pete. Confessions of a Spy: The Real Story of Aldrich Ames. G.P. Putnam's Sons, New York. 1997.

Eco, Umberto. The Role of the Reader. Indiana University Press, 1979.

Ehrenraus, Peter. "Silence and Symbolic Expression." Communication Monographs, v. 55, pp. 41-55. 1988.

Fenster, Mark. Conspiracy Theories: Secrecy and Power in American Culture. University of Minnesota Press, 1999.

Fish, Stanley. There's No Such Thing as Free Speech, and It's a Good Thing, Too. Oxford University Press, New York. 1994.

Goodnight, Thomas, & John Poulakos. "Conspiracy Rhetoric: From Pragmatism to Fantasy in Public Discourse." Western Journal of Speech Communication, v. 45, pp. 299-316. Fall 1981.

Goodwin, Irwin. "Physicists Refute Charges that Icons Helped Soviets Build Nuclear Bomb." Physics Today, v. 47, pp. 59-62. June 1994.

Habermas, Jurgen (transl. Maeve Cooke). On the Pragmatics of Communication. MIT Press, Cambridge. 1998.

Halperin, Morton, and Hoffman, Daniel. Top Secret: National Security and the Right to Know. New Republic Books, Washington D.C., 1977.

Handberg, Roger. "Know Thy Enemy: Changing Images of the Enemy in Popular Literature."

Havill, Adrian. The Spy Who Stayed Out in the Cold: The Secret Life of FBI Double Agent Robert Hanssen. St. Martin's Press, New York. 2001.

Haydock, Robert. "Some Evidentiary Problems Posed by Atomic Energy Security Requirements." Harvard Law Review, v. 61, pp. 468-491. 1947.

Haynes, John Earl and Klehr, Harvey, Venona: Decoding Soviet Espionage in America. Yale University Press, New Haven CT. 1999.

Hirsch, Daniel, & William Mathews. "The H-Bomb: Who Really Gave Away the Secret?" Bulletin of the Atomic Scientists, v. 46, pp. 22-30. Jan/Feb. 1990.

Hofstadter, Richard. The Paranoid Style in American Politics and Other Essays. Alfred Knopf Press, 1965.

King, Robert. "Treason and Traitors." Society, v. 27, pp. 39-48. July/Aug. 1989.

Lane, Christel, and Richard Bachmann, eds. Trust Within and Between Organizations: Conceptual Issues and Empirical Applications. Oxford University Press. 1998.

Lear, Floyd Seyward. Treason in Roman and Germanic Law. University of Texas Press, 1965.

Lee, WenHo, and Zia, Helen. My Country Versus Me. Hyperion, New York. 2001.

Liebeskind, Julia Porter, & Oliver, Amalya Lumerman. "From Handshake to Contract: Intellectual Property, Trust, and the Social Structure of Academic Research." In Lane & Bachmann's Trust Within and Between Organizations, Oxford University Press, 1998.

Los Alamos Historical Society. Los Alamos: The First Forty Years. Los Alamos, NM. 1984.

Maas, Peter. Killer Spy: The Inside Story of the FBI's Pursuit and Capture of Aldrich Ames, America's Deadliest Spy. Warner Books, New York. 1995.

MacDonnell, Francis. Insidious Foes: The Axis Fifth Column and the American Home Front. Oxford University Press. 1995.

Markle, Donald. Spies and Spymasters of the Civil War. Hippocrene Books, New York. 1994.

Marnell, William. The Right To Know: Media and the Common Good. Seabury Press, New York. 1973.

Martin, Robert. The Free and Open Press: The Founding of American Democratic Press Liberty, 1640-1800. New York University Press, New York. 2001.

Melanson, Philip. Secrecy Wars: National Security, Privacy, and the Public's Right to Know. Brassey's Inc., Washington D.C., 2001.

Merton, Robert & Lazarsfeld, Paul. "Mass Communication, Popular Taste, and Organized Social Action." in The Communication of Ideas, ed. Lyman Bryson. Harper, New York. 1948.

Model, Peter. "The Spies Who Came In for the Gold." Wilson Library Bulletin, v 66, pp. 61-64. May 1992.

Moynihan, Daniel Patrick. Secrecy: The American Experience. Yale University Press, New Haven. 1998.

Newman, James. "Control of Information Relating to Atomic Energy." Yale Law Journal, v. 56-5, pp. 769-802. May 1947.

Newman, Robert. Owen Lattimore and the "Loss" of China. University of California Press, Berkeley. 1992.

Nussbaum, Martha. Poetic Justice: The Literary Imagination and Public Life. Beacon Press, Boston MA. 1996.

Pasternak, Douglas. "Squeezing Them, Leaving Them: Defectors say Washington isn't Good about Keeping its Word." U.S. News & World Report. July 8, pp. 12-16. 2002.

Pincher, Chapman. Traitors: The Labyrinths of Treason. Sidgwick & Jackson, London. 1987.

Powe, Scot. "Espionage, Leaks, and the First Amendment." Bulletin of the Atomic Scientists, v. 42, pp. 8-10. July 1986.

Ransom, Harry Howe. The Intelligence Establishment. Harvard University Press, Cambridge MA. 1970.

Robertson, Ken G. Public Secrets: A Study in the Development of Government Secrecy. St. Martin's Press, New York. 1982

Rudgers, David. Creating the Secret State: Origins of the Central Intelligence Agency, 1943-1947. University Press of Kansas, 2000.

Sarbin, Theodore, Ralph Carney, and Carson Eoyang, eds. Citizen Espionage: Studies in Trust and Betrayal. Praeger, Westport CT. 1994.

Scott, Robert. "Rhetoric and Silence." Western Journal of Speech, v. 36, pp. 146-158. 1972.

Shuy, Roger. Language Crimes: the Use and Abuse of Language Evidence in the Courtroom. Blackwell Press, Cambridge MA. 1993.

Shuy, Roger. Bureaucratic Language in Government and Business. Georgetown University Press, Washington DC. 1998.

Snyder, John. "The Spy Story as Modern Tragedy." Film Reader, v.3, 1978, pp. 216-234.

Stafford, David. The Silent Game: The Real World of Imaginary Spies. University of Georgia Press, 1991.

Stober, Dan, and Hoffman, Ian. A Convenient Spy: WenHo Lee and the Politics of Nuclear Espionage. Simon & Schuster, New York.. 2001.

Taussig, Michael. Defacement: Public Secrecy and the Labor of the Negative. Stanford University Press, 1999.

Taylor, Bryan. "Organizing the 'Unknown Subject': Los Alamos, Espionage, and the Politics of Biography." Quarterly Journal of Speech, v. 88, p. 33-49. 2001.

Theoharis, Athan, editor. A Culture of Secrecy: The Government versus the People's Right to Know. University Press of Kansas, Lawrence KS. 1998.

Trice, Harrison & Beyer, Janice. "Studying Organizational Cultures Through Rites and Ceremonials." Academy of Management Review, v. 9, pp. 653-669. 1984.

Trulock, Notra. Code Name Kindred Spirit: Inside the Chinese Nuclear Espionage Scandal. Encounter Books, San Francisco. 2003.

U.S. House of Representatives, 106th Congress. House Permanent Select Committee on Intelligence Report of the Redmond Panel "Improving Counterintelligence Capabilities at the Department of Energy and the Los Alamos, Sandia, and Lawrence Livermore National Laboratories. Report 106-687, U.S. Government Printing Office. February 2000.

Vise, David. The Bureau and the Mole: The Unmasking of Robert Philip Hanssen, the Most Dangerous Double Agent in FBI History." Atlantic Monthly Press, 2001.

Wang, Jessica. "Science, Security, and the Cold War: The Case of E.U. Condon." Isis, v. 83, pp. 238-269. 1992.

Weiner, Tim. Betrayal: The Story of Aldrich Ames, an American Spy. Acacia Press, Los Angeles. 1995.

Weinstein, Allen, & Vassiliev, Alexander. The Haunted Wood: Soviet Espionage in America-- the Stalin Era. Random House, New York.. 2000.

Whately, Richard (ed. Douglas Ehninger). Elements of Rhetoric: Comprising an Analysis of the Laws of Moral Evidence and of Persuasion, with Rules for Argumentative Composition and Elocution. Southern Illinois University Press, Carbondale. 1828, 1963.

Wise, David. Molehunt: The Secret Search for Traitors that Shattered the CIA. Random House, New York. 1992.

Wise, David. Nightmover: How Aldrich Ames Sold the CIA to the KGB for $4.6 Million. Harper Collins, New York. 1995.

Wise, David. Spy: The Inside Story of How the FBI's Robert Hanssen Betrayed America. Random House, New York. 2002.

Wilson, Veronica. "Elizabeth Bentley and Cold War Representation: Some Masks Not Dropped." Intelligence and National Security, v. 14-2, pp. 49-69. Summer 1999.

"Reform in the Classification and Declassification of National Security Information: Nixon Executive Order 11,652." Iowa Law Review, v. 59, pp. 110-143. 1973.

Society, July/Aug. 1986. Special Issue on Scientific Freedom.