

Heritage Lectures

No. 705

May 18, 2001

INTELLIGENCE AND ESPIONAGE IN THE 21ST CENTURY

THE HONORABLE RICHARD SHELBY

I appreciate the opportunity to speak to this distinguished group on a topic that is a critical part of my responsibility as Chairman of the Senate Select Committee on Intelligence.

In the four years I have served as Chairman, the Committee has held more hearings on issues relating to counterintelligence and security—from PRC nuclear espionage and the loss of missile technology to China to the Hanssen case—than any other single issue.

This should not come as a surprise. Spying has been described as the world's "second oldest profession"—and one that is, in the words of one former CIA official, "just as honorable as the first."

Espionage has been with us since Moses sent agents to spy out the land of Canaan and the Philistines sent Delilah to assess Samson's vulnerabilities. And spies are with us today. I will not attempt to cover the history of espionage from Biblical days to now, but I would like to take the opportunity to address some important recent history, and lessons from recent history, as well as some of the issues and challenges, new and old, that we face as we address counterintelligence in the 21st century.

Let me emphasize at the outset that due to the extremely sensitive nature of the subject, and the

fact that some of the matters I will discuss are the subject of ongoing investigations, I will be speaking for the most part in very general terms.

The first point I would like to make is that, as those of you who follow counterintelligence are well aware, between the peaks of public attention that attend the arrest of an Ames or a Hanssen, or a case like the Wen Ho Lee case, there is a quiet but steady parade of espionage or espionage-related arrests and convictions.

A July 1997 Defense Security Service publication lists more than 120 cases of espionage or espionage-related activities against the United States from 1975 to 1997. And those are just the ones that got caught.

HERITAGE FOUNDATION
LECTURE
held May 9, 2001

Produced by
Kathryn and Shelby
Cullom Davis Institute
for International Studies

Published by
The Heritage Foundation
214 Massachusetts Ave., NE
Washington, DC
20002-4999
(202) 546-4400
<http://www.heritage.org>



ISSN 0272-1155

This paper, in its entirety, can be
found at: [www.heritage.org/library/
lecture/hl705.html](http://www.heritage.org/library/lecture/hl705.html)

Since then, we have had the Peter Lee case; the Squillacote and Trofimoff cases; David Boone, an NSA employee; Douglas Groat, who pled guilty to extortion against the CIA in a plea bargain in which espionage charges were dropped; the conviction of INS official Mariano Faget of spying for Cuba; and, of course, the Hanssen case. Counterintelligence success or failure is often a matter of lessons learned or not learned. For today's purposes, I would like to concentrate on some lessons from the most damaging and high-profile recent cases: Ames, PRC espionage against our nuclear and missile programs, and the Hanssen case.

THE AMES CASE: A COUNTERINTELLIGENCE DISASTER

In its investigation of the Ames case, the Senate Intelligence Committee found a counterintelligence disaster. Elements of this disaster included: a crippling lack of coordination between the CIA and the FBI, fundamental cultural and organizational problems in the CIA's counterintelligence organization, a willful disregard of Ames's obvious suitability problems, failure to coordinate and monitor Ames's contacts with Soviet officials, failure to restrict Ames's assignments despite early indications of anomalies, deficiencies in the polygraph program, deficiencies in the control of classified information, and coordination between the CIA's security and counterintelligence operations. Most disturbing was the CIA's failure to pursue an aggressive, structured, and sustained investigation of the catastrophic compromises resulting from Ames's espionage, in particular the destruction of the CIA's Soviet human asset program as a result of Ames's 1985 and 1986 disclosures.

By 1986, it was clear to the CIA that, as the SSCI report on the Ames matter concluded, "virtually its entire stable of Soviet assets had been imprisoned or executed." Yet as a result of the failure to mount an effective counterintelligence effort, it was another eight years before Ames was arrested. The FBI, which lost two of its most important assets following Ames's June 1985 disclosures, also bore responsibility for the failure to mount an adequate counterintelligence effort, as a 1997 report by the

Department of Justice Inspector General made clear.

These two FBI assets, who were KGB officers, and a third KGB asset were betrayed by Hanssen in October 1985—just a few months after all three names were disclosed by Ames, according to the Justice Department affidavit in the Hanssen case. The two KGB officers were later executed; the third asset was arrested and imprisoned. Also extremely disturbing, from my perspective, was the egregious failure by both the CIA and FBI, over the course of Ames's espionage, to inform the congressional oversight committees, despite the clear statutory obligation to notify the committees of "any significant intelligence failure."

While the committees obviously would not have been in a position to investigate the compromises themselves, they would certainly have exerted pressure that would have resulted in greater management attention and a more sustained effort that could have led to a more expeditious resolution.

Before leaving the Ames matter, I should point out that failure also may come from learning the wrong lessons. Most notably, many of the CIA's failings in the Ames case can be traced to an overreaction to the "excesses" of the Angleton years, which thoroughly discredited the CIA's counterintelligence program, particularly in the Soviet-East European Division of the Directorate of Operations, where Ames worked.

CHINA STEALS NUCLEAR SECRETS

Turning next to Chinese espionage against the Department of Energy and U.S. nuclear weapons programs: unlike in the Ames case, extensive investigations into the compromise of U.S. nuclear weapons information have failed to resolve all the key questions.

That there was espionage, there is no doubt. As the April 1999 Intelligence Community Damage Assessment of PRC nuclear espionage concluded, "China obtained by espionage classified US nuclear weapons information." What is not yet known is how, and from whom, the Chinese got this information. As a result, we do not know enough of the

story to attempt a final or definitive exercise in counterintelligence “lessons learned.”

At the same time, a great deal is known about the overall security and counterintelligence problems at the DOE labs, which have been amply documented, for example in the report of the President’s Foreign Intelligence Advisory Board. Because this is so well known, I will not touch upon it in detail, but will only make a few general observations. First, despite the history of espionage against the nuclear labs—and the obvious value of U.S. nuclear information to any nuclear power, whether established, emerging or aspiring—the Department of Energy’s counterintelligence program did “not even meet minimal standards,” in the words of the director of the program in November 1998.

He testified that “there is not a counterintelligence [program], nor has there been one at DOE for many, many years.” This was a terrible failure of counterintelligence analysis and practice—and of common sense.

Moving from DOE to the role of the FBI, it is abundantly clear that the FBI counterintelligence investigation into the W-88 compromise lacked resources, motivation, and senior management attention; failed to pursue all relevant avenues of potential compromise; and was characterized by a number of missed opportunities. The CIA, for its part, failed to assign adequate priority or resources to the translation of the documents provided by the now-famous walk-in source.

But let me be clear: While the investigation and prosecution of Wen Ho Lee that emerged from the W-88 investigation have been widely criticized, we should not lose sight of the facts. Dr. Lee illegally, purposefully, downloaded and removed from Los Alamos massive amounts of classified nuclear weapons information—the equivalent of 400,000 pages of nuclear secrets, representing the fruits of 50 years and hundreds of billions of dollars worth of research. Now I would like to address the Hanssen case.

INVESTIGATING THE HANSSSEN CASE

Robert Philip Hanssen was arrested on February 18. On March 5, the Senate Intelligence Committee directed the Department of Justice Inspector General to conduct a review of the Hanssen matter. On March 7, the Committee authorized a separate Committee investigation. Because of the ongoing criminal investigation and pending prosecution, I cannot go into details of Hanssen’s alleged activities beyond what has already been made public by the FBI and the Department of Justice.

By the way, there is a great deal of information in that affidavit—too much information, some have suggested—and for anyone interested in counterintelligence, it is a fascinating and chilling story. Because there is much that is not yet known about this case, it would be premature for me to offer any definitive comments or lessons learned.

What I will do is identify some of the questions and issues the Committee is investigating, and offer a few preliminary and personal observations.

First the Committee will prepare a factual summary of the Hanssen case outlining his FBI career and alleged espionage activities. An important question here, since the Justice Department affidavit describes only espionage activities from 1985 through 1991, and 1999 through February 2001, is explaining what may or may not have been an eight-year gap in Hanssen’s activities.

We also need to know if he was involved in any activities of concern prior to 1985. The Committee will examine whether there were counterintelligence warning flags indicating a penetration of the FBI—for example, source reporting or unexplained compromises of human sources or technical programs—and the response of the counterintelligence community, if any, to these events.

This is a critical issue. The 1997 Department of Justice Inspector General report on the Ames case criticized the FBI for failing to mount an intensive counterintelligence effort to pursue evidence of catastrophic damage to the FBI’s and CIA’s Russian operations beginning in 1985.

The signs were there, but the FBI did not pursue them in an aggressive and systematic fashion. We now know that such an effort might have detected Hanssen, as well. We will look closely at the FBI's efforts following the 1997 IG report to see if the agency applied these lessons from the Ames investigation to its ongoing counterintelligence efforts.

There have been press reports of other source information or counterintelligence analyses that might have pointed to Hanssen sooner. I cannot address those reports; I can only say that we are reviewing both Ames-era and post-Ames reporting and analysis to determine whether any relevant warning flags were missed.

Moving to Hanssen himself, the Committee will review possible warning flags in Hanssen's own behavior that raised, or should have raised, questions about his loyalty or suitability, and the response, if any, by Hanssen's colleagues and security personnel.

FBI internal security procedures during the period of Hanssen's activities will be another critical focus of the Committee's work. The Committee will review personnel security issues, such as the FBI's failure to adopt an across-the-board polygraph program comparable to those at the CIA and NSA, and the adequacy of financial disclosure requirements.

The Committee will look hard at the FBI's computer and information systems security practices, and at Hanssen's computer activities, including the possibility that he gained unauthorized access or might have manipulated FBI computer systems. Another issue is the control of classified information in general. Hanssen appears to have been able to gain authorized or unauthorized access to an extremely wide range of sensitive intelligence programs and activities, many of which may have been beyond his "need to know." (Ames too was able to gain access to a great deal of information for which he had no need to know.)

This problem may be FBI-wide, and not limited to Hanssen. In the 1987 ANLACE report—the first of several inconclusive efforts to solve the 1985 Ames/Hanssen compromises I described earlier—FBI agents found that as many as 250 FBI employ-

ees in the Washington Field Office alone had knowledge of these highly sensitive cases. Also, I am concerned that Hanssen was able, according to the affidavit, to provide the KGB with original documents (rather than copies), pointing to a serious failure in document control.

These security issues also are the subject of Judge Webster's investigation. We look forward to the results of the Webster Commission, which should aid the Committee in making budgetary and other decisions to enhance security at the FBI.

The impact of Hanssen's alleged espionage on operational, budgetary, and programmatic decisions across the Intelligence Community goes to the heart of the Committee's responsibilities and will be a critical component of our review. The key issues include: what operations, programs and sources were compromised, and their remaining utility, if any; how much it will cost to replace or replicate these capabilities, if it can be done at all; and the impact of the compromise on the utility of these collection capabilities against other, non-Russian targets. The Committee will review the possibility that Moscow used sources or programs compromised by Hanssen for "perception management" purposes.

In the wake of the Ames case, the CIA concluded that the Soviets and later the Russians had used controlled sources or information compromised by Ames to manipulate U.S. assessments of issues ranging from internal Soviet political developments to Soviet and Russian military capabilities and Russian policy toward the former Soviet republics.

In sum, the Committee will collect the facts, identify shortcomings and failures in the FBI's internal security and counterintelligence operations that may have facilitated Hanssen's alleged activities, determine the impact on the U.S. government's intelligence collection efforts, and take such legislative or other steps as appropriate.

The Committee also will review possible changes in law to facilitate the investigations and prosecution of espionage cases. This process may take some time, as the final assessment of the Hanssen case will not be completed for some time, even if

Hanssen were to reach a plea agreement tomorrow. In the meantime, we intend to take preliminary steps, as appropriate, in this year's intelligence authorization bill.

DIFFICULT QUESTIONS ABOUT HANSSEN

Let me offer a few general thoughts on the Hanssen matter, reiterating that these are personal and preliminary in nature. First, let me restate the obvious question: How did the nation's premier counterintelligence organization fail to detect a spy in its midst for 15 years? While a number of explanations have been and will continue to be offered, it is difficult to avoid returning to that simple question. In any case, we intend to find out the answer. Part of the answer may lie in Hanssen's ability to use his knowledge of FBI activities and techniques to avoid detection.

While some of the early assessments of Hanssen as a master spy may have been exaggerated, it is clear that he was in a position to benefit from his inside knowledge of FBI procedures, and that would explain at least some of his success in evading detection for so long. On the other hand, it seems fair to say that Hanssen, like Ames, benefited from the FBI's failure aggressively to pursue the source of the 1985 agent losses and other compromised FBI activities, as documented by the Justice Department IG.

Second, why didn't the FBI do more to take advantage of the lessons that the CIA learned so painfully from the Ames case with respect to financial disclosure, compartmentation, an effective polygraph program, and other security and counterintelligence measures? Granted, the reforms adopted by the CIA post-Ames could not have stopped Hanssen in time to prevent grave damage to the national security because Ames's arrest and the subsequent recriminations and reforms came almost a decade after Hanssen appears to have started spying. On the other hand, we may well learn that additional losses could in fact have been avoided had Hanssen been caught five years earlier.

A RESTRUCTURED NATIONAL COUNTERINTELLIGENCE SYSTEM

I would now like to move to an important development in national-level counterintelligence policy.

On December 28, 2000, President Clinton signed a Presidential Decision Directive entitled "U.S. Counterintelligence Effectiveness—Counterintelligence for the 21st Century," or "CI-21." President Bush has proceeded to implement the directive. CI-21 reflects the concerns of senior counterintelligence officials—which the Committee shared—over the ability of existing U.S. counterintelligence structures, programs, and policies to address both emerging threats and traditional adversaries using cutting-edge technologies and tradecraft in the 21st century. I am pleased to say that the Senate Intelligence Committee, on a bipartisan basis, played an important role in keeping the pressure on the executive branch to force them to come up with a counterintelligence reform plan even when the executive branch process bogged down amid interagency disagreements.

From an analytical perspective, CI-21 restates and expands upon other recent assessments of the emerging counterintelligence environment. It recognizes that the threat has expanded beyond the traditional paradigm of "adversary states stealing classified data"—which includes traditional espionage by Russia, the PRC, and others—to include new efforts by these traditional adversaries, as well as certain allies and friendly states, to collect economic information and critical but sometimes unclassified technologies, as we have seen just recently in the Lucent case.

A key element of this threat is the growing use of modern technology, particularly modern computer technology and the Internet, to develop information warfare (IW) and intelligence collection capabilities and intelligence tradecraft that alter traditional notions of time, distance, and access.

Faced by these emerging challenges, the drafters of the CI-21 plan found current U.S. counterintelligence capabilities to be "piecemeal and parochial," and recommended adoption of a new counterintelligence philosophy—described as more policy-

driven, prioritized, and flexible, with a strategic, national-level focus.

CI-21 also established a restructured national counterintelligence system. Key elements of the plan include a proactive, analytically driven approach to identifying and prioritizing the information to be protected, enhanced information-sharing between counterintelligence elements, and more centralized guidance for counterintelligence policies and resources.

CI-21 proposes significant changes in the way the United States government approaches, and organizes itself to meet, the threat of foreign espionage and intelligence gathering. The Committee looks forward to working with the new Administration to ensure the effective implementation of the CI-21 plan.

THE CHALLENGE FOR THE NEW CENTURY: THINKING THE UNTHINKABLE

In closing, I would like to make a couple of general points about the challenge of counterintelligence in the 21st century.

The first is the impact of technology. Modern microelectronics and information technology have revolutionized just about everything else, so it is not surprising they would have an impact on counterintelligence. After all, the currency of espionage is information. Therefore, the impact of evolving information technologies is particularly significant.

One aspect of this is the miniaturization of information. It took Jonathan Pollard 17 months to spirit away enough classified documents to fill a 360 cubic foot room.

Today, that information can fit in a pocket, dramatically diminishing the risk of detection while increasing the productivity of an agent. A laptop computer like the one that disappeared from the State Department can fit into a briefcase or backpack yet yield an entire library of information.

Another is the revolutionary change in the dissemination of information. Depending on the computer security measures in place, an agent can

transfer or simply retype classified information into an unclassified e-mail system and send it around the world in seconds.

Or consider the “virtual dead drop.” No more marks on mail boxes or hiding messages in a soda can. Classified information can be transferred or retyped into an unclassified computer with an Internet connection, and left there for someone to “hack” into. The whole transaction may be difficult or impossible for security officials to detect or recreate. Even if the agent is careless and fails to delete classified information from an unclassified computer, it may be difficult if not impossible to prove anything beyond a security violation.

Another challenge, in an era of extensive scientific cooperation between nations that are, if not adversaries, not exactly friends, is the difficulty of protecting sensitive, proprietary, or even classified information in the course of scientific exchange or joint ventures. This problem was especially apparent in the interactions between American and Chinese engineers launching U.S. satellites in China that were the subject of an Intelligence Committee investigation.

American satellite company engineers, who have multimillion-dollar payloads riding on primitive Chinese rockets, face a serious conflict of interest: how to ensure successful launches while not doing anything to improve Chinese rockets that are essentially identical to Chinese ICBMs in everything but the payload. Identifying sensitive, but unclassified, technical information at risk in transactions of this type, and then finding ways to protect it, will be an important focus of the CI-21 plan.

Most fundamental to counterintelligence—as true today as ever—is the need to “think the unthinkable.” Yet this is one of the most difficult attitudes to instill and maintain because it runs contrary to human nature, especially in open societies like the United States.

Consider the following scenarios: Two Soviet agents are named by an American President to serve as Secretary of State and Secretary of the Treasury.

Unthinkable? You might think so. Yet Henry Wallace, Vice President during Franklin Roosevelt’s

third term, said later that if Roosevelt had died and he had become President, he would have appointed Laurence Duggan and Harry Dexter White—both of whom were revealed to have been Soviet agents—to those positions. As it happened, Harry Truman replaced Wallace three months before Roosevelt's death.

Or imagine that another Soviet agent became chief of the British Secret Intelligence Service, or SIS. Yet Kim Philby was one of the main contenders to take over the SIS before he came under suspicion and eventually defected. (And there are still people who claim that Roger Hollis, head of the British internal security service MI-5, was a Soviet agent.)

Today, thinking the unthinkable is not getting any easier, but it is just as critical to our national security.

As we proceed to face the counterintelligence threat of the 21st century, we are faced with a host of challenges: some new, others ancient and deeply rooted in human weakness, and some not yet even invented.

I am pleased to say that today we have an Administration that is more willing to see the world as it is, and not as we would wish it, and this gives me confidence in our ability to meet these challenges. I look forward to working with the Bush Administration to build on the lessons of the past, and seize the opportunities of the present and future, to strengthen our national counterintelligence policies and posture in defense of our nation's security.

—*The Honorable Richard Shelby, a Republican, represents Alabama in U.S. Senate and serves as Chairman of the U.S. Senate Select Committee on Intelligence.*