Espionage: Why Does it Happen?

By Lynn F. Fischer

DoD Security Institute

The Department of Defense and the Intelligence Community have been taking a hard look at the possible causes of espionage and the betrayal of public trust. The results of systematic research have important implications for protecting the nation's secrets and critical technologies.

Since World War II, perhaps going back to the time of the Rosenberg case (Ethel and Julius Rosenberg, convicted of espionage for passing atomic secrets to the Soviets, were executed in 1953.) there has been a lot of conventional wisdom about why people commit espionage and what personal characteristics might be clear predictors of involvement in this crime. Views on this subject have changed over the past several decades, but only recently have federal agencies begun to engage in serious research regarding its root causes or reliable indicators.

At one time, it was commonly believed that ideology, particularly of the communist brand, was behind the thinking of espionage offenders. And in fact, during the 1950s a number of spies were communist sympathizers. Another bit of conventional wisdom held that most were foreign implants, that is deep- cover agents or moles, and therefore might be spotted by their Slavic accents, foreign associations or odd way of dress. And then there were those who were convinced that many spies were homosexuals, a connection recently downplayed by former Secretary of Defense Cheney as "an old chestnut." By the 1980s, it became evident that most spies were volunteers rather than foreign agents or Americans recruited by foreign agents. And in recent years, security educators have promoted the theory that nearly all of these offenders did it for money -- for greed or because they were faced with overwhelming financial problems.

A call for policy based on scientific evidence:

Interestingly enough, one can find examples from the history of espionage in the United States that seem to confirm any of these theories, particularly the latter. On the other hand, there are cases that contradict any preconception about who would be a bad security risk. In determining whom we can trust to protect our secrets, what guidelines are appropriate? Should personnel security policy be based on common sense or in what appears at the time to be self-evident truth? In a major turning point, the 1985 Stilwell Commission Report called for such policies to be grounded on hard evidence and the scientific method:

"Adjudication policies also beg for a firmer basis in research. DoD guidelines for denying security clearances should logically be based upon a credible analysis which demonstrates a logical link between the grounds used for denying a security clearance (e.g., excessive use of alcohol) and the likelihood that such behavior may reasonably be expected to lead to a compromise of classified information."

The report went on to call for more funding for security research in a number of areas including "determining the efficacy of the elements of background investigations, including information

required on personal history statements and in subject interviews." Consider the historical context of this report: By 1985, the number of new espionage cases coming to light were nearly a dozen a year, not the least of which was the Walker Spy Ring and the untold damage in its wake. Many of the culprits arrested held high level security clearances. Political leaders and the press were seriously questioning the effectiveness of our security clearance procedures.

Responding to the Stilwell challenge:

The Stilwell recommendation did happen. By 1986, PERSEREC, the Personnel Security Research Center in Monterey, California, with several full-time government researchers and contract support was up and running. One of PERSEREC's first research efforts was to develop an unclassified database on all Americans involved with espionage against the U.S. since World War II based on media reports, trial records, and unclassified official documents.

One might ask how a massive accumulation of facts about these espionage offenders would bring us closer to an understanding of this crime and what causes it. We knew a lot about each individual case from detailed investigative reports that followed the event. But it was difficult to make sound generalizations about this type of behavior without data on a wide range of variables for as many cases as possible. One of the things that made a rigorous study of espionage somewhat difficult was that, despite its tremendous damage, classic spying on behalf of a foreign intelligence service is a relatively rare crime. Since 1945 to the present there have been fewer than 120 acknowledged espionage cases which have appeared in open sources.

But even with fewer than 120 cases, an existing database of information has made it possible to systematically collect, quantitatively code, and statistically analyze basic information. This includes such things as personal background, the methods and motivations of the offender, and pertinent facts about the crime itself -- situational features, what was lost or compromised, and consequences for the subject. For example, we might want to know what sort of people have been arrested, why they did it, how they got involved, what if anything they were paid, or what foreign interest received (or was intended to receive) the information.

Answers to these and many other questions are included in PERSEREC's May 1992 report, "Americans Who Spied Against Their Country Since World War II". That report analyzed 117 cases, the number in the database as of June 1991. This report shows for each of 56 variables (such as age, gender, occupation, or motivation) the percentages of individuals who fall into one of several categories.

Some examples of the report's statistical analysis follow. These tables allow us to examine the frequency distribution for one variable at a time or to make comparisons among variables. The inclusion of a large number of cases is important in research of this type since the larger the number of cases we can observe, the greater is our confidence in the generalizations we can make on the subject.

The example below illustrates one way in which these data are displayed in the PERSEREC report. We can see here that by far the greater number of offenders initiated the activity themselves (usually by contacting foreign representatives). Of the remainder, fewer than a fourth were recruited by foreign intelligence agents.

Volunteers and Recruited Spies

Volunteers and Recruits	%	N
Volunteers	62.9	73
Recruited by family or friends	14.7	17
Recruited by foreign intelligence	22.4	26
Total	100.00	N = 116
		Missing = 1

It is also possible to spell out the relationship between two variables with a cross-tabulation. The table below shows that among espionage offenders who were in the military, about two-thirds began their involvement before the age of 30, while among civilians; initial offenders tended to be older. This difference probably is a result of the simple fact that the military opulation has a lower average age, but it does remind us that security awareness products used in military organizations should appeal to younger adults.

Age Espionage Began by Military and Civlian

	Military		Civilian	
Age	%	N	%	N
20	8.3	5	1.8	1
20-24	38.3	23	17.9	10
25-29	20.0	12	21.4	12
30-34	13.3	8	14.3	8
35-39	13.3	8	10.7	6
40-44	6.7	4	17.9	10
45+	0.0	0	16.1	9
Total	100.0	60	100.0	56
Median	25.3	32.6		
N = 116				
Missing - 1				

Perhaps the most important section of the PERSEREC report looks at motivations for espionage cross-tabulated with other variables. Were, for example, volunteer spies seeking other rewards than recruited offenders? The table below compares three categories of spies with regard to reported motivations:

Motivation of Volunteer and Recruited Spies

	Volunteers		Recruited by Family or Friends		Recruited by Foreign Intell.	
Motivation	%	N	%	N	%	N
Money	59.6	56	29.2	7	45.2	14
Ideology	8.5	8	25.0	6	22.6	7
Disgruntlement/Revenge	18.1	17	4.2	1	9.7	3
Ingratiation	6.4	6	41.7	10	0.0	0
Coercion	0.0	0	0.0	0	12.9	4
Thrills/Self-importance	7.4	7	0.0	0	9.7	3
Total	100.0	94	100.0	24	100.0	31
N = 150*						

*More than the number of spies because there were 34 spies with multiple motivation

According to this evidence, financial gain played a much larger role among volunteers (almost 60%) than among those who were recruited. Not surprisingly, those recruited by family or friends were more often motivated by ingratiation (the desire to favor or satisfy) than by anything else. However,

it must be pointed out that at least 34 spies out of the total had mixed motives for what they did, and in those cases, it is often difficult to determine which driving force was dominant.

Although money appears to top the list of motivations attributed to these offenders by the report, it is interesting to see (as shown in the following chart) how few received any significant amount of payment for these activities before being arrested. Almost half received nothing because of early detection or because they acted from non-mercenary motives. Only ten received $100,000 or more -- usually paid over long periods of time. This is important information for the security educator to communicate to employees. In most cases, the financial pay-off to the espionage offender is nil or next to nothing, when compared to the monumental cost to the nation from compromised weapon systems, lost technology lead- time, or neutralized intelligence collection systems.

Estimate of Money Received

Amount	N
None	46
$50-1K	10
$1K-10K	11
$10K-100K	17
$100K-1M	7
$1M+	3

N = 95 Missing = 22

Here are a few additional highlights from the report's tables and descriptive findings that give us additional understanding about motivations and situational factors:

-- The percentage of offenders who were volunteer spies (not recruited) has increased sharply each decade since the 1950s, reaching 79% in the 1980s.

-- Forty offenders out of the total number had close foreign relatives, and spies with foreign relatives were much more likely to have been recruited by foreign agents than those who had none.

-- Money tops the list of apparent primary motivations for espionage with 52%. Others include ideology (18%), disgruntlement or revenge (15%), ingratiation (9%), coercion (4%) and thrills or intrigue (3%). But money as a motivation can mask much more complicated motives.

-- Ideology was the dominant motive in the 1940s (12 cases); there have been only nine cases based on ideology since then.

-- Out of 117 individuals, 6 were homosexual, 86 heterosexual, and the sexual orientation of the remaining 25 was unknown. The report states that homosexuality was not a significant factor in any of the cases.

-- Thirty-nine offenders were known to have been involved in drug or alcohol abuse; those who were intercepted before information was lost were more likely to be substance abusers.

-- Volunteer spies were more likely to fail in their effort to pass information to foreign interests. Forty- four percent were caught in the act whereas only 7% of the recruited spies were intercepted before they could damage national security.

Any of these findings may have implications for both policy and security awareness activities. The fact, for example, that since 1945 a large number of former spies had foreign family connections suggests that employees with foreign emotional ties should be informed that adversarial intelligence services have in the past used this as a leverage for recruitment. But overall, the predominance of volunteer spies (as compared to recruited sources) should lead us as security educators to stress the importance of continuing evaluation at least as much as, if not more than, recruitment modus operandi of foreign agents. Another example from the PERSEREC study, worth promoting to our employee populations, is that the high percentage of offenders who were also substance abusers (out of proportion to the general employee population) suggests that drug use and alcoholism should be taken very seriously as an indicator having implications for security.

There are of course many other interesting percentage distributions and comparisons between variables that may shed light on espionage and how to combat it. For one thing, it may now be possible to compare espionage with similar betrayal of trust behaviors -- embezzlement, white-collar crime, industrial espionage, computer crime, or police corruption. This raises the question: Is espionage a really unique type of wrongdoing committed by quite different types of people or is it just one variation of betrayal-of-trust behavior? The verdict is still out on that question. And, on the policy side, with this database we can check out specific propositions about situational or personal traits such a drug use, alcoholism, or sexual misconduct as possible indicators of security risk. This information may eventually help to validate or downgrade the importance of specific investigative criteria used as the basis for granting clearances.

PERSEREC's Espionage Database is being updated and its holdings expanded. As new cases are added to the file and previously missing data filled in, the database becomes increasingly valuable as an information resource to the security community. In a related research effort, PERSEREC analysts are now compiling a much larger collection of cases related to the illegal export of critical technology to foreign interests.

Espionage research from another perspective

The PERSEREC effort to decipher the mysteries of espionage is not the only research activity of its type which is providing valuable results. At the other end of the continent, in Newington, Virginia, several federal agencies have pooled their resources to support the Community Research Center. The CRC as a research effort has actually been going strong for several years under the name "Project Slammer", but only recently has it acquired full-time staff members and permanent office-space.

The driving concept behind Slammer is that if we want to know why people commit espionage, we should ask those who have done it. In other words, understanding the behavior by going directly to the perpetrators for information. On the surface, this is a simple idea, but as a research method for collecting valid information there are a number of hurdles to overcome. One of them is that most of these offenders are in maximum security prisons (hence the name, "Project Slammer") and some are unwilling to talk . Of the thirty who have agreed to be interviewed to date, each has participated in several hours of psychological testing and in-depth discussions with one or more clinical psychologists and counterintelligence specialists associated with the project. Using both standard interview forms and recorded videotapes, interviewers have recorded information on a wide variety of personality, behavioral, and situational factors as well as on espionage tradecraft. Each full interview is taped and coded for later retrieval when specific research questions need to be answered.

There are several important differences that separate the Slammer project from PERSEREC

activities. For one thing, the former is dedicated exclusively to the study of espionage behavior and its causes. For PERSEREC, espionage research is only one of many projects related to the entire field of personnel security. (A selected listing of PERSEREC research reports which can be ordered is included in this issue.) A second important distinction is that while PERSEREC's findings rest on the statistical analysis of quantitative data on a large number of variables or indicators, Project Slammer seeks valid conclusions from a qualitative, in-depth case study analysis of information on a smaller (but continually growing) selection of offenders. And when thoroughly dissected, these studies may tell us more about the intricate psychological factors, perceptions, and emotions leading to the tragic decision to betray one's own country. An important part of each data set is drawn from the individual's recall of childhood events and pre-adult behavior that tell us a lot about his psychological and emotional development and mental health.

These in-depth Slammer studies can also tell us about the situational context in which espionage was committed. For example, what was going through the mind of an offender at the time: Did he consider the probability of detection, was he aware of penal consequences if caught, did he see anything standing in the way of this action in the workplace, and what were his immediate objectives for resorting to this act?

To date, the research staff at Project Slammer has issued a number of reports -- many of them are highly technical or classified -- which makes it impossible to discuss their content here. In addition, much of the published output has been developed to address counter-intelligence or investigative issues not specifically of interest to the security educator or cleared employee. However, copies of Project Slammer reports will soon be available also through the Defense Technical Information Center and will be announced in the Security Awareness Bulletin. Report topics will include psychological profiles of individual spies, why people commit espionage, monitoring and continuous evaluation, evaluation of suitability criteria, and managing at-risk employees.

The Countering Espionage Video Series

What may be of greater interest to those of us who are committed to security education and awareness is a parallel effort by the CRC to develop, in conjunction with the Department of Defense Security Institute, a series of video products. These videos are based (as is the research effort) on the recorded testimony of convicted espionage felons in which they reveal their thinking and personal suffering. The Countering Espionage series has already produced one award-winning product, "You Can Make a Difference," and several more are nearing completion. The second one to be released, "It's Not a Victimless Crime," will concern the personal damage done by espionage to the offender and to his family members.

In these video productions we are attempting on one hand to dispel misconceptions, and on the other, to motivate and empower all employees and service personnel to get involved in the continuing evaluation process by intervening on behalf of troubled co-workers when they see signs of extreme stress or other indicators. The argument here is that intervention may take the form of personal confrontation, counseling, employee assistance programs, or reporting in confidence to a security professional. Whatever response is most appropriate, each of us has a personal responsibility to act in the interest of a friend or co-worker who is showing signs of not being able to cope with an immediate situation or life-crisis. This idea is very similar to the admonition that "friends don't let friends drive drunk." In this context, our message is "don't let friends or co-workers become so vulnerable that they might resort to some desperate act."

Working toward a Theory of Espionage

Will it ever be possible to predict with any degree of accuracy who might commit espionage? Perhaps not, but through research we are moving to a much better understanding of the motivations or causal factors which entrap people into this web of crime. According to Dr. Neil Hibler, Project Slammer Director, our hope for the future is that we at least will be able to identify "at risk" individuals before or during employment, thus preventing espionage or compromise by cost-effective policies which are at the same time harmonious with human values and constitutional principles.

For the present we must try to make some sense out of the sizable array of information collected on these cases by both the PERSEREC and Slammer research efforts. At first assessment, the facts seem to defy our efforts to generalize about motivations or causes. It could almost be said that each instance of this crime is a unique event in itself -- each has its own twists and exceptional personalities. Each account reveals another variation on the old theme of personal failure and betrayal.

However, CI professionals and psychologists working on the Slammer data tell us that common patterns are beginning to emerge. The results of psychological testing and interviewing disclose that they frequently encounter two, almost opposite, personality types among these 30 offenders under study -- one, a highly manipulative, dominant and self-serving type; the other, passive, easily influenced and lacking in self-esteem. Anyone who is at all knowledgeable about recent cases will immediately think of spy ring organizers such as John Walker and Clyde Lee Conrad as typical of wheeler-dealers. Walker's son, Michael, comes to mind as a likely candidate for the wimp category. Project Slammer researchers tell us that by far the larger number of former spies in their sample fall into the first group, but contrary to what we might expect, none of the subjects studied entered a position of trust with the intention of committing espionage.

We also learn from CRC's report on personality characteristics of espionage offenders [soon to be available from DTIC] that a frequent trait among this group is obsessive self-centeredness or selfishness - - a lack of genuine caring for others and an indifference to problems experienced by other persons.

But the larger issue is this: What would lead even a person who is lacking in a basic sense of loyalty or sympathy for others to opt for espionage, which most of us would conclude is a highly risky and ultimately self-destructive act? The answer is complex, but we can make sense of what is going on. These researchers are finding that in case after case they are looking at a person who is psychologically vulnerable to begin with and whose judgment under stress may be severely impaired. Following employment in a sensitive position, and when confronted with a high level of emotional pain, frustration, or anger, in desperation he or she resorts to espionage as a way out or as a solution to a problem. It may be a one-time act such as the theft of a single CIA manual by William Kampiles, or repeated acts of betrayal over months or even years, as reported in the case of former Army Warrant Officer James Hall.

The nature of the espionage offender's vulnerability to involvement in this crime, or any other damaging behavior, differs from case to case. We do know that several of these people were victims of severe child abuse which resulted in an intense self-esteem problem. Others appear to have been raised without the benefit of moral training or positive role models. In his cell at the Federal Penitentiary at Lewisburg, Pennsylvania, Michael Walker told us:

"...my father got me involved in espionage through years of careful grooming. The way you train a man to think, a young man to think about values, morals, and things like that. These are important. If

you can convince your child that certain things are okay, they're more inclined to break certain rules in society."

Does this mean that anyone who has emerged from a dysfunctional or undesirable family background is going to attempt espionage? Definitely not. The idea driving this project was to try to understand why those who have committed this crime went in that direction when they found themselves in what they believed to be an intolerable situation. The "crisis" or compelling circumstance in the lives of these offenders turns out to be as varied as the origins of their vulnerabilty or predisposition to destructive behavior. Several individuals faced mounting debts and personal bankruptcy, some craved professional recognition, one was a covert homosexual who bitterly resented military policy. In another case, Thomas Dolce, an Army civilian employee with a history of psychiatric problems directly links his espionage activity with domestic tragedy:

"I had seen a psychiatrist off and on for about three years. I had been in, not a psychiatric hospital, but in a psychiatric wing of a general hospital three or four times. I had been on some heavy medication and so on. I was a real mess for about three years. Roughly two years after that, for whatever that means, is when all of this started -- shortly before or shortly after this [espionage activity] started -- I'm not sure which, but my mother died very suddenly. And I think that I did not fully appreciate at the time just what the impact of that was. I think I've come to appreciate that more in the last year -- the impact that it had on me. Roughly a year after my mother died, my late wife was diagnosed as having cancer. And we both suffered with that for about three years before she died. It was during those three years that the bulk of the activity took place."

As with psychological vulnerability, these findings should not suggest that employees confronted with a life-crisis will necessarily select espionage, or any self-destructive act as an option. But on the other hand, they are at much greater risk. It is important to emphasize again that, by comparison with other felonies, espionage doesn't happen that often. We know that only a tiny fraction of people under stress -- who think they are up against the wall -- would even think of espionage as a remedy for anything. Call it basic loyalty, patriotism, or morality; in most cases, overriding values would rule it out. However, for those few who did go over the line, this new research also shows that they rarely considered themselves to be disloyal. We can assume that this rationalization is related to their typical, self-centered view of life.

Long-term benefits from research on espionage

Then how will the results of these research ventures described above assist us in protecting the nation from the loss of critical information and technology by theft, negligence or betrayal? First, in the area of initial screening for access to classified or sensitive information, we stand to learn in the future a lot more about what makes an individual vulnerable, or a higher risk, and what does not. Much of the on-going work of both PERSEREC and the Community Research Center is related to the evaluation of the current investigative criteria for suitability to hold a clearance -- foreign connections, drug abuse, sexual misconduct, illegal activities, etc.

Each of these complementary research efforts is in its own way providing insight into aspects of the larger issue of predicting human reliability in government personnel security programs. For example, while both research projects report a high incidence of habitual and excessive drug and alcohol use among espionage offenders (clearly a suitability issue), Project Slammer researchers call attention to their data which indicate that substance abuse was not typical of offenders during the time they were in a position of trust. It may have happened before or after.

Secondly, and this may be the more immediate benefit, in the area of prevention following the granting of access: The chief conclusion drawn from several of the Slammer reports is that had procedures been in place to help vulnerable employees deal with personal crisis, including an organizational climate supportive of co-worker intervention, much of this damage would have been prevented. As related by former CIA employee William Kampiles, even something as simple as personal counseling might have deflected him from his single but extremely damaging criminal act:

"...if someone outside that office had sat me down and...just said, listen this is a talk. You can say whatever you want. Nothing to hide. Nothing will leave this room. Tell us what's going on in your life, because there's obviously a problem. You're not doing well, you know, you're not communicating in a positive manner. Your relationships with your co-workers are bad... what's going on?...we don't think that this is what you want. It's not what's been demonstrated in the past in your life. Is there anything that we can do to help?"

Research Impact: Of immediate importance to security education

Lastly, for the security educator, much is to be gained from keeping fully informed about what espionage research has to tell us. "Findings" that are clear and easy to understand, such as the fact that most of the damage in recent years has been the result of volunteer U.S. citizens rather than recruited or foreign spies, is useful information to plug into awareness briefings. And as mentioned earlier (based on the PERSEREC study), the potential extra vulnerability of employees with foreign relationships, and the high incidence of substance abuse in the offender population are pertinent issues to discuss in briefings and open forums.

Project Slammer findings offer us some of the best verbal ammunition available for promoting the concept of co-worker responsibility and continuing evaluation. Through these research efforts, we are learning that people who have fallen into the trap of espionage are like the guy in the next office or the trusted technician on the assembly line. As mentioned earlier, no offender studied so far has entered into a position of trust with the intention of betraying that trust. Among convicted Americans who had held a clearance, involvement with espionage happened following initial employment, sometimes years later.

This focus on the active role of rank-and-file employees in preventing espionage is reinforced by another revelation: Many of the former spies claim that their decision to commit this crime was based in part on their belief that the probability of being noticed and reported by co-workers was next to nothing. In other words, the messages for our audiences to hear are: Intervene in the interest of an at-risk employee before he or she becomes a threat to national security. And secondly, a workplace in which people are known to be aware and willing to take action when appropriate presents a powerful deterrent to espionage.

Through security education, we also need to clear the deck of misconceptions. Not the least of these is the idea that reporting in confidence about a co-worker is going to be detrimental to that person. Several of the former spies, such as William Kampiles, have said that they wish someone had stood in their way. Statements like this help support our arguments that personal intervention is morally and ethically justified as being consistent with the interest of a co-worker who is exhibiting signs of distress or the inability to cope with a situation.

These central themes are developed in the Countering Espionage video series. And as these products are released, our employee populations will have the opportunity to witness for themselves the

testimony of former spies. Through comprehensive security awareness programs -- briefings, videos, newsletters, posters and other visual reminders -- we can create a climate in which people are sensitive to trouble signs and feel morally empowered to act. And at the same time we are building a deterrent atmosphere where the potential offender will assess the chance of detection as too high.

Over all, the credibility of our personnel security programs depends upon a great "selling-job" by the security educator through effective briefings and other communications. And our credibility as communicators and educators stands to be greatly enhanced each time we are able to say, "What we are telling you is not just common sense, but this has been validated by scientific research."