Naval War College Review

Volume 41
Number 4 *Autumn*

Article 7

1988

The Security Dilemma

E. D. Smith Jr.
U.S. Navy

The Security Dilemma

Captain E. D. Smith, Jr., U.S. Navy

When one is ingenious, he can obtain secret information about everything.
Sun Tzu, c. 400 B.C.

We should begin by recognizing that spying is a fact of life . . . .
Ronald W. Reagan, 29 June 1985

Safeguarding classified or sensitive information in an open democratic society is extremely difficult. With over 4 million individuals having access to classified material, the likelihood that some of this material will be provided to our enemies, through error or design, must be considered very high.[1] The Walker spy case demonstrated that serious damage to our security can be caused by a few individuals with access to sensitive information. The Walker spy ring was comprised of retired Navy Warrant Officer John Walker; his brother Arthur Walker—a retired lieutenant commander; his son, Navy Seaman Michael Walker; and a retired senior chief radioman, Jerry Whitworth. Spanning a period of at least 18 years, this ring of spies, orchestrated by John Walker, freely provided a wide variety of classified material to the Soviet Union for monetary compensation. They were finally caught, arrested and sentenced in 1985, following an FBI investigation of the claims by John Walker's former wife that he had been a spy for years.

Of significance in this case was the fact that Walker and his cohorts were not caught by the security "system" they operated within—the various rules, procedures, and practices established for the control and safeguard of classified material. If Barbara Walker had not come forward, it is doubtful we would know about Walker's activities—considered by many to be the most damaging ever uncovered.

Captain Smith holds the Edwin T. Layton Chair of Naval Intelligence and serves as the staff intelligence advisor, the head of the intelligence division of the Operations Department, and the War College Special Security Officer. He is a graduate of the University of Connecticut and holds a master's degree in international relations from the University of Southern California.

While the documents and publications provided to the U.S.S.R. by the Walker ring were significant disclosures, the most serious damage probably resulted from the sale of cryptographic key material to the Soviets, which may have allowed them to read our classified message traffic and decrypt our secure voice circuits over a 15 to 18-year period. Although we will never know with certainty all of the messages that the Walker ring gave the Soviets access to, the testimony of a Soviet KGB defector, Vitaly Yurchenko (who subsequently redefected to the U.S.S.R.) indicates that over a million messages were involved.[2] One million messages equates to over 150 messages per day for 18 years, so if Yurchenko's statements are true, the Walker "take" was truly a gold mine for Soviet intelligence. As the Director of Naval Intelligence has testified, the Walker spy ring provided the Soviet Union with information that would have had ". . . powerful war winning implications. . . ." if war had broken out during the period of their espionage activities.[3]

After the early revelations of the Walker case, which generally coincided with the arrest and subsequent trials of the major participants, professional military interest in the case focused on the damage assessments in an attempt to understand what had been passed to the Soviets and then to determine what we could do about it. The Navy took several administrative steps that included the much publicized 50-percent reduction in security clearances, tightening up on "need to know" requirements for access to classified material, establishment of standards and investigative requirements for security and communications personnel, and reduction of classified holdings and other measures designed to improve security controls.[4] In June 1985 (Walker was arrested in May 1985), the Department of Defense Security Review Commission (informally known as the Stilwell Commission after its chairman, General Richard G. Stilwell) was chartered by Secretary of Defense Caspar Weinberger "to conduct a review and evaluation of Department of Defense security policies and procedures."[5] Their report and recommendations were duly submitted on 19 November 1985.

That the Walker case was not an isolated incident of espionage was proven immediately after the Stilwell Commission made its report, by the arrest of another Navy spy, John Jay Pollard, on 21 November 1985. Pollard, a naval counterintelligence analyst, was charged with selling classified documents to the Israelis. In the following year we learned about the case of Marine PFC Clayton Lonetree and other U.S. Marine guards who were alleged to have allowed Soviet agents to enter the U.S. Embassy in Moscow and possibly other locations. These cases suggest that we should be cognizant of, and continually concerned about, the possibility of espionage being committed by U.S. citizens.

The issue here is that, in spite of the real damage sustained by us from these espionage cases, we simply do not seem to be seriously concerned about

the necessity for stringent security measures. Three years after the promulgation of the Stilwell Commission's report and the introduction of some of the security-related measures indicated above, it appears we have reverted to a "business as usual" approach to security. That is to say, we are doing little about it. The impact of the Security Awareness briefings that were required in the aftermath of the Walker investigation has faded along with the interest of our commanders. The inconvenience of searching personnel for classified material when they depart our ships or facilities has resulted in curtailment of that security measure, even in commands that profess a serious concern for security enforcement. Uncontrolled use of copy machines continues unabated at most naval commands, and limited access to classified material based on "need to know" is rarely practiced. While there are individual commands and senior officers who are convinced of the threat and have actively pursued or imposed security measures within their span of control, these efforts appear to be the exceptions, not the rule. Mere adherence to the administrative "letter of the law" is not enough to protect national security. We need regulations and procedures that are effective, practical, and universally understood throughout the Navy and other branches of the military.

Effective security is difficult to develop and implement. That which enhances security generally has a negative impact on efficiency. Incoming traffic is detained when ID cards are checked at base entrances. The search of briefcases taken out of secure facilities may cause pedestrian traffic jams. If classified documents are found in a briefcase, the subsequent investigation takes time and manpower, both of which are often in short supply. A security-related operation, like any other operation, requires the use of assets. However, unlike some other operations, there is no identifiable payoff for security enforcement and there is usually no real proof that the time and manpower spent on security have been effective. This is one reason why we pay lip service to directives on security while searching for ways to ease the impact of these directives on our commands.

In many instances, the execution of security measures carries with it the implication that we cannot trust one another. All of the 4 million or so individuals with security clearances have transacted a personal contract with the U.S. Government stating that they will safeguard the classified material to which they are given access. As Americans, the idea that someone we know will betray that trust is abhorrent to us. We would no more consider our fellow workers to be potential spies than we would consider our neighbors to be potential murderers. In general, we trust people and, as has been demonstrated in the Jonathan Pollard espionage case, we are reluctant to report our suspicions of fellow workers, even when the evidence is overwhelming. Pollard was a civilian intelligence analyst working in the Navy's Anti-Terrorist Alert Center. A fellow worker had observed him

removing large quantities of classified material from his office over a period of several months. The co-worker finally became suspicious after hearing a security awareness lecture about the Walker case and reported his suspicions to the Naval Investigative Service (NIS). Based on this tip, NIS agents put Pollard under surveillance and observed him taking classified intelligence documents from his office to his car for subsequent transfer to the Israeli Embassy. A joint NIS-FBI investigation led to Pollard's arrest in November 1985 and conviction for espionage in March 1987. Significantly, the fellow worker who provided the "tip" on Pollard reportedly turned down an offer of a cash reward because he did not want it known that he had informed on his co-worker.

Given these predilections and the large number of people with access to classified material, what can we realistically do about security? First we must decide whether or not there is a real and significant security problem. A scan of the public record on foreign intelligence presence in the United States, along with a sampling of recent espionage cases within the Navy, indicates that, in fact, there is a security problem of massive scope.[6] In the words of former Assistant Secretary of Defense Richard Perle, "The free world today is confronted with the most audacious, well-run campaign in modern history of illegal trade diversions, espionage and the acquisition of publicly available material."[7]

The first step in countering this problem is recognizing it. The Stilwell Commission attempted to do this by examining current DOD security practices and making recommendations for improvement. Because of either resource constraints or bureaucratic inertia, we have not followed through on those recommendations. Some of them deserve a closer look.

In developing a plan of attack, we should look for measures that are both effective—that promise some payoff for enhanced security—and practical. To be practical, the measures must be manageable, within reasonable costs, and have a low or minimal impact on the overall operation of the facility. Keeping all classified documents locked in a safe would be the most effective means of security, but not very practical. On the other hand, although posting signs about security would be inexpensive, with minimal negative impact on the facility operations, its effectiveness is doubtful. The measures we seek lie somewhere in between.

We might want to start with the Walker case and particularly with the *modus operandi* of the principal participants. While stationed at COMSUBLANT in Norfolk, John Walker used a Minox camera to photograph documents at his desk. At other times, he took documents home to be photographed. He has stated in testimony that had he been subjected to the possibility of a random search while leaving the base, he would not have attempted to take classified material home. Jerry Whitworth and Michael Walker routinely walked off their ships with classified documents.

In Michael's case, the quantities of classified material he removed were often large. If either of these individuals had been subjected to a search on the quarterdeck before departing, their actions might have been deterred.

Random searches of briefcases and other containers being taken from facilities where classified material is stored can be an effective deterrent to blatant espionage. Such searches will not detect all thefts of classified material, but the possibility of discovery will serve as a deterrent. The Stilwell Commission recommended that all briefcases and personal belongings be subjected to search upon both entry and exit from DOD installations.[8] While searching all containers might be more effective than random searching, facilities with high densities of personnel may find this impractical. From the standpoint of deterrence, a thorough search of random individuals may, in fact, be more effective than cursory searches of all personnel. Random searches conducted throughout facilities having unguarded or multiple exits will also increase the risk of discovery.

In order to properly conduct the confiscation of unauthorized classified material, should it be discovered, procedures must be promulgated, and security personnel must be trained. Normally, this should include taking the individual and the confiscated physical evidence to a nearby room for an initial investigation by the facility security officer or NCO. If, after further examination of the situation, a purposeful security violation is considered likely, the case should be turned over to the local NIS office for action. (Of interest, in the Pentagon, checks of briefcases and other containers are made only on the way in; no checks are made on the way out.)

In a similar manner, random searches of vehicles departing naval bases can also be conducted under the same kind of ground rules. Discovery of classified material in the custody of an individual without a valid courier card should be considered reason enough to turn the case over to the local NIS office for further investigation. Such searches are not needed weekly, nor with any particular periodicity. It is the randomness of the search that creates a risk to the would-be spy.

Random searches appear to be both effective (as a deterrent) and practical (low cost, with minimal impact on the operation if conducted properly). While the Director of Navy Security Policy told a Congressional committee in 1985 that the Navy had been asked "to beef up their random inspection of papers and articles carried by personnel entering or leaving Naval commands,"[9] personal observation suggests this is not being done universally. Some commands and facilities that implemented random search programs have discontinued them after receiving complaints. A certain amount of inconvenience should be tolerated when the payoff is enhanced security.

Another potential tool in reducing security leaks is the polygraph examination. While the effectiveness of the polygraph has been the subject

of debate, NIS considers it to be ". . . an excellent deterrent to those considering involvement in espionage-related activities, and . . . another means of indentifying persons who have already committed themselves to such activity."[10] Polygraph examinations will continue to be used for individuals with access to particularly sensitive information, but there is no way that the limited number of qualified polygraphers currently employed by the Defense Department can examine all 4 million clearance holders. This fact was recognized by the Stilwell Commission, which concluded, nevertheless, that "It would also be desirable . . . for persons cleared at the SECRET and TOP SECRET levels to face the possibility of a randomly administered polygraph examination at some time during their careers."[11]

Since a major expansion of the polygraph program is unlikely, we should develop more practical alternatives. A program for random security interviews with personnel who have access to the more sensitive categories of classified material, such as those with top secret clearances, could provide the same deterrent effect. The interviews could be done periodically by NIS or command security personnel, with the names of individuals to be interviewed drawn randomly from a list of cleared personnel—as has been done with random drug urinalysis. The questions could be the same as those posed during the security polygraphs, that is, directed specifically to counterintelligence issues.[12] The function of this interview, as in the case of random searches, would be to deter. While the hardened or trained spy is unlikely to confess to espionage under simple, straightforward questioning, such interviews may provide the basis for further investigation of either the interviewed individual or his fellow workers.

The effectiveness of a random security interview program is dependent upon the interrogative skills of the interviewer, but the very existence of such a program should act as a psychological deterrent. The assets required to conduct such a program are minimal; one interviewer for a few hours per month or quarter. As a measure to enhance security it seems to be both effective and practical.

Since both of the security measures suggested are designed primarily to deter, they should be advertised and promulgated for full impact. The third suggested measure is a security awareness program, one that provides personnel with an understanding of the security threat posed by a variety of foreign intelligence organizations, as well as a general understanding of the security program and procedures in force at their installation or facility. A key recommendation of the Stilwell Commission was that DOD improve the quality of such programs.[13] A Senate committee examining the espionage threat came to a similar conclusion, adding that such programs are often insufficiently tailored to the needs of their audiences. As the committee report stated, "the usefulness of such material is illustrated by the fact that once the U.S. Navy began to improve its security awareness briefings, after

the Walker case, co-workers of Jonathan Pollard noted his unusual [illegible] of document requests and alerted authorities."[14]

Naval commands are currently required to receive an "operations security" briefing once annually. Unfortunately, these briefings are often *pro forma* lectures which meet the administrative requirement without really enhancing the command's understanding of the nature of the threat. The security manager at each facility should develop a security awareness program tailored to the needs, location, and circumstances of his command. Such briefings need not be boring and can include case studies of real situations that personnel will relate to.

When reading about the Walker case and the ease with which the participants were able to operate, many people wonder why the principals in that case were not caught earlier by "the system." How was Michael Walker able to leave the U.S.S. *Nimitz* carrying large quantities of classified documents? Why was Jerry Whitworth never questioned about his extravagant life-style? The fact is, procedures for handling classified material are easy to subvert from within unless everyone is involved. As the Director of Naval Intelligence has testified, "The ultimate vulnerability of cryptosystems and all procedures designed to protect sensitive information lies at the human level. . . . No system ever designed can be invulnerable to the corrupt, cleared individual who has access . . . we depend on an individual's integrity and deterrence of the law to ensure that this trust is fulfilled."[15]

In addition to the security awareness program outlined by the Stilwell Commission, which would primarily describe the security threat from foreign intelligence services, their *modus operandi*, and appropriate case studies of actual examples, the security awareness program should also include information about the facility security program. Since the primary intent of a random search and a random security interview program is to deter, the programs will need to be described. Deterrence works only if the threat is understood. Discussing these procedures openly, in the context of an overall security awareness program, should also make personnel aware of the need for such measures and, hopefully, lessen their resentment of the inconvenience they may suffer as a result of these measures.

Part of this program should focus on the classic, behavioral profiles of a spy and patterns of activity which should trigger suspicion on the part of fellow workers or supervisors. While these "indicators" are not observed in every espionage case, they do provide a general set of guidelines for activity that warrants a second look. The classic indicators include: unexplained affluence or major change in financial status; attempts to gain unauthorized access to classified material (beyond legitimate need to know); removal of classified material from the facility; and unexplained or regular foreign travel.[16]

Another part of a security awareness program should focus on what to do if our people suspect that they have been approached by foreign intelligence personnel or have suspicions about other facility personnel or procedures. A "spy" hotline, similar to the DOD Hotline for Fraud, Waste and Abuse, offers a simple, inexpensive, and practical solution. The telephone numbers of facility security personnel and the local Naval Investigative Service office should also be widely promulgated.

As security measures go, the security awareness program is probably the most important. It promotes personal responsibility for security, bringing it to the human level, explaining why people should be concerned, what they should look for, and what they can do about it. As indicated above, it can also set the stage for further active security measures, such as random searches and interviews. It is important, however, that security awareness not be considered a short-term goal. Would-be traitors and spies will always be with us; the threats they pose deserve continued and aggressive actions to keep security awareness visible.

Command involvement is the key to ensure that attention to security is a continual process. The Stilwell Commission report recognized this and one of their findings concluded that "The key to genuine improvement in DOD's security posture is continuing, pervasive oversight by commanders and supervisors at all levels."[17] Commanders and supervisors who support command security programs, becoming personally involved in developing security measures tailored to their commands' requirements, demonstrate to their subordinates the necessity for taking the security system seriously. This is vital to the success of any security-related program.

The three security measures outlined above—random searches, random interviews, and a security awareness program—provide the core for an active security program that is both effective and practical. Until the Navy or DOD directs the implementation of these or similar measures, the security of our classified information is being left basically to individual commands and organizations. As the Walker case amply demonstrated, the impact of espionage operations is not solely contained in the command where the spying originated. Indeed, in the Walker case, the effect was and continues to be felt worldwide. If we are to get serious about protecting classified information and preventing future Walkers or Pollards from operating, we need to change our attitudes towards security and not only recognize the threat, but do something about it. Implementing the measures outlined above would be a beginning.

Notes

1 U.S. Congress, Senate, Committee on Armed Services, Subcommittee on Manpower and Personnel, *The National Security Protection Act of 1985*, Hearing (Washington: U.S. Govt. Print. Off., 1985), p. 13.

2. U.S. Congress, Senate, Select Committee on Intelligence, *Meeting the Espionage Challenge: A Review of United States Counterintelligence and Security Programs*, Report (Washington: U.S. Govt. Print. Off., 1986), p. 103.
3. *Ibid.*, p. 98.
4. U.S. Congress, House, Subcommittee of the Committee on Government Operations, *Counterintelligence and National Security Information*, Hearing (Washington: U.S. Govt. Print. Off., 1985), p. 93.
5. U.S. Department of Defense, *Keeping the Nation's Secrets: A Report to the Secretary of Defense by the Commission to Review DOD Security Policies and Practices*, (Washington: U.S. Govt. Print. Off., 1985), p. 113.
6. House Subcommittee of the Committee on Government Operations, pp. 80-91.
7. U.S. Congress, Senate, Permanent Subcommittee on Investigations, Committee on Governmental Affairs, *Foreign Missions Act and Espionage Activities in the United States*, (Washington: U.S. Govt. Print. Off., 1985), p. 73.
8. U.S. Department of Defense, p. 11.
9. House Subcommittee of the Committee on Government Operations, p. 93.
10. *Ibid.*, p. 40.
11. U.S. Department of Defense, p. 11.
12. House Subcommittee of the Committee on Government Operations, pp. 90-91.
13. U.S. Department of Defense, pp. 68-69.
14. Select Committee on Intelligence, p. 5.
15. *Ibid.*, p. 98.
16. *Ibid.*, pp. 118-119.
17. U.S. Department of Defense, p. 14.

ψ

Conference on Soviet Military Doctrine in an Era of Change

Old Dominion University is sponsoring a conference on "Soviet Military Doctrine in an Era of Change" for academics and defense professionals at Old Dominion University on 25-27 May 1989. For further information, contact: Philip S. Gillette, Graduate Program in International Studies, Old Dominion University, Norfolk, Virginia 23529-0088; (804) 440-4643.