William Scott Malone 1/22/89

The ~~exmd~~ Outlook article in today's Washington Post ("Code Name Catastrophe") ~~in today's Washington Post~~, coauthoredwith William Cran, who I do not know, is my first knowledge that Scott stopped preferring to be known only as Scott. The Post says they are Emmy-award-winning producers for PBS' 'Frontline.'" This is my first knowledge that Scott had won an Emmy.

I met him under unusual conditions and thereafter he spent some time here.

Throughout 1975 Group Health Assn. physicians had ignored the pain syptoms I had been reporting, telling me I was getting old. Ignored it until pain was excrutiating. In about September I was there in great pain and was told to walk less than a block to George Washington University Hospital. As I left the doctor's office I passed a pay phone and told Jim Lesar that I would try to make my way down to the front door on Penna. Ave., NW and signal a cab - to take me less than a block. I asked him to phone Lil and tell her. I did, with pain and difficulty, get to the street and sat on a wall in front of the building trying without success to signal a cab. (Thrombophlebitis)

After some time a tall young man I'd never seen before came up to me and introduced himself, saying that Jim had sent him to see if he could help me. I asked him to go inside the building and see if he could commandeer a wheelchair. He emerged with one and pushed me first to the admitting office of the hospital and then to the room to which I was assigned. I gave him money with which to buy me a bottle of Scotch and a carton of cigarettes. He returned with both and returned my money. Instead of getting the J & B Scotch I'd asked him to get he'd gotten what he said (not incorrectly) was better even that Chivas Regal, Royal Ages. He was still with me when, during the physical examination, the phone rang. It was the lecture bureau asking about the debate I was to have with David Belin at Vanderbilt. The examination on the phone ring was prostate! Scott told them I'd call back and I did.

He was then in his ~~senior~~ junior year at George Washington and one of a group of students from there and particularly Maryland who came here often.

The next summer he spent some time here, working on my files, painting, talking with me, and what I did not discover until after much misfiling, staying close to drunk and drunk. He was unable to avoid raiding my liquor and when there was nothing left but a bottle of blackberry wine I'd gotten to keep for medicinal purposes, one night after we retired that disappeared.

His father was a retired Army colonel. The family lived or had a place of business in Alexandria. When Scott moved out and into his own apartment we gave him an over-stuffed chair that was too large for us and a recliner I was replacing and probably a few other things. He came up less frequently then but I'd hear from him from time to time. He quit college within days of getting his degree.

Soon I heard that he was freelancing with foreign and domesstic TV producers. Then he undertook a delicate and I thought unwise secret task for the House Select Committee on Assassinations, an activity I considered improper for the Congress. He came up here with a thin (at least for that era) tape recorder designed to fit inside a man's inside jacket pocket and not be seen. It was shaped like cigar cases used to be shaped, thin enough so that only thin cigars could fit in that space. He played me tapes he'd made while talking to prominent people in the mob who did talk to him. As I recall he also did some clandestine taping in Canada. I remember some of the names but think there is no need to record them. It coild have been very dangerous. and it was a futility, meaningless. He'd listened to me about other things but not this.

I have no idea what, if any, influence on him the time he spent with me had and what I told him meant to him, if anything.

(The debate with Belin was held, I was released too soon and inadequately prepared for the trip, with no cautions at all, and fortunately another student, Floyd Lamore,

of the University of Maryland, insisted on going with me. By the morning after the debate I wasn't able to get a shoe on my left foot. The airline ticket agent at the airport took one look at me and got a wheelchair and single-loaded me on a back seat then sent a passenger who was a nurse back to sit with Floyd and me. Belin had gotten an advance copy of Post Mortem from a Congressman to whom I'd given it and was the half way through it. He and we left Nashville on a Friday and after that debate and his reading Belin held a Saturday press conference to call for a new investigation of the JFK assassination. I had several other scheduled appearances and speeches in that period and Floyd accompanied me on several others although they turned out not to be too difficult physically.)

The PBS documentary Scott coproduced is to be aired Tuesday 1/24. ("The Spy Who Broke the Code")

Code Name Catastrophe

How Moscow Cracked Our Secret Cipher Systems

Post 1/22/89

By William Scott Malone and William Cran

THE COLD WAR between the United States and the Soviet Union may be winding down, but the spy war between them continues. And there's new evidence that America may have suffered greater damage in this secret war than is generally recognized.

The Soviets appear to have obtained access to the most deeply held U.S. secret of all—the codes used to protect our sensitive government messages. U.S. intelligence and law-enforcement officials say they base this analysis on a careful review of the 1985 John Walker spy case, which leads them to two disturbing conclusions:

■ The United States hasn't caught all the Soviet code spies. More Walkers are probably out there, still undetected. Investigators reached this judgment because of indications that Moscow had other, and perhaps better, sources of U.S. "crypto" secrets than the Walker spy ring.

■ The Soviets have broken some supposedly "unbreakable" cipher systems. Investigators believe that by piecing together technical information provided by Walker and his associates, the Soviets have been able to

See SECRETS, D4, Col. 1

William Scott Malone and William Cran are Emmy-award-winning producers for PBS' "Frontline." They spent almost a year investigating the Walker case for the upcoming "The Spy Who Broke The Code," which will air next Tuesday on PBS.

SECRETS, From D1

replicate U.S. hardware and read at least some of our secret message traffic—a feat that U.S. officials once believed was impossible.

A sign of America's continuing espionage problem came during the past month, with the arrest of U.S. Army Warrant Officer James W. Hall III in Georgia and former Navy chief petty officer Craig D. Kunkle in Virginia. Kunkle, who was arrested during an FBI sting operation two weeks ago, didn't actually pass secrets to the KGB, so he isn't believed to have caused any real damage. But Hall's alleged espionage, if true, was of a far more damaging nature. As an Army signals-intelligence specialist, Hall had access to super-secret U.S. cryptographic machines and keylists, more commonly known as codes and ciphers.

The Walker case showed just how vulnerable these code systems are. John A. Walker Jr., a onetime Navy warrant officer, spied for the KGB for almost 20 years before he was arrested in May 1985, after his ex-wife turned him in to the FBI. Walker had recruited his brother, his 20-year-old son and his best friend into his spy ring.

"It was the greatest case in KGB history," former KGB defector Vitaly Yurchenko told his American debriefers in 1985. "We deciphered millions of your messages. If there had been a war, we would have won it."

"K-Mart has better security than the U.S. Navy," Walker told us during a series of interviews last August for a PBS "Frontline" documentary on the Soviet espionage threat. He noted that he used to tell his partner, Jerry Whitworth, that selling U.S. secrets "was a buyers' market."

What worries Phillip Parker, the former FBI deputy assistant director for counterintelligence who supervised the Walker case, is that the KGB's handling of Walker demonstrated that he was not their most important agent. "He was just another messenger boy," says Parker. "There are no doubt other John Walkers still out there," agrees a National Security Agency (NSA) official.

From Walker's very first visit to the Soviet Embassy in Washington in December 1967, it was obvious the Soviets were intimately familiar with America's top-secret codes. When Walker, at that first meeting, presented a copy of a Navy keylist stamped "Top Secret Specat [Special Category]," the KGB security officer immediately wanted to know why there was no "Letter of Promulgation" signature on the back of the keylist. It took the startled spy a few moments to realize that the NSA had recently discontinued the signature practice.

As with the famous Sherlock Holmes case in which the crucial clue was a dog that *didn't* bark, the most important thing about the Walker case may be the questions the KGB didn't ask him. "I can only deduce that they were getting their information from somewhere else," Walker eventually concluded.

"The NSA boys went pale when I told them about the Russians not wanting anything on the [then most advanced machines]. It meant that it had already been compromised," says Walker. Such a conclusion offers perhaps the most disturbing implication for U.S. security, since a new generation of U.S. code machines had begun to go into service by the early 1980s with the Air Force, Army, Navy and NATO.

To assess the damage done by Walker and the other spies, it's necessary to understand a bit about the arcane science of cryptology. Experts say there are two basic elements to a modern code system: the logic and the key. The humming, Navy-gray code machines contain what is in essence an electronic formula (or algorithm) called the logic. The key is a list of numbers and letters that set the machine and tell the logic formula when to commence. To maximize security, U.S. keylists are changed every 24 hours.

The machines themselves, along with their associated "technical manuals," while closely guarded, are usually not top-secret, because they are distributed around the world and their designers assume they will eventually be lost or stolen. The NSA has long presumed that no machine by itself could be used to read a coded message—without that day's keylist. Keylists thus become the object of intense classification and protection.

"In the context of communications information, the keylist is considered the ultimate," recalled Walker's convicted cohort Jerry Whitworth in an interview for the "Frontline" documentary. "The only other thing that's better would be the keylist, tech manual and the equipment. Then you've got the whole shebang."

"Obviously you can't steal the equipment," explains Walker, "so the next best thing would be to give them the technical manual. From the technical manual, you can build the equipment by a process of [reverse] engineering."

Walker did just that. Using a Minox camera, he supplied the Soviets with all the technical manuals he could lay his hands on. "They got the original technical manuals from me and I provided them with amend-

COMMONWEALTH MAGAZINE

John Walker with electronic equipment in 1983 before his arrest as a Soviet code spy.

ments [and] modifications to that equipment as they occurred over the years," says Walker. "When Mr. Whitworth took over, he continued to provide those changes basically to the [KWR-]37 and to the [KW-]7" code machines.

The Soviets still needed the daily keylists, but Walker, and later Whitworth, kept them amply supplied. Whitworth let his pride show when discussing a $10,000 bonus Walker paid him for providing "months" of continuous keylists. "The bonus thing came up over a period of having years of consistency—not months, but years," he says.

The NSA had thought that even if this sort of breach occurred, the damage would be limited. Earl David Clark, the former chief of NSA's Office of Communications Security, testified during Whitworth's trial in 1986: "We design our systems [so] that without a key, we are highly confident that no one can read these communications . . . . You would only be able to exploit those communications for which you have that logic [tech manual] and keying material in which those communications were encrypted. [You] could not read tomorrow's traffic if [you] didn't have tomorrow's key . . . ."

Clark's confidence may have been misplaced. According to Navy officials, the internal design logic of some machines was indeed compromised by the Walker spy ring, and the Soviets were able to read secret U.S. messages without the keylists. Adm. James D. Watkins, then chief of naval operations, obliquely acknowledged the compromise during a June 1985 press briefing. According to Watkins, loss of the cryptographic logic designs was "the most serious area of compromise. Some technical design communications information has probably been lost."

Four months later, after Walker began cooperating with damage-assessment officials, then Navy secretary John Lehman was more specific: "We assume that the Soviets were able to compromise the design logic of some of the cryptographic ma-

chines, which would enable them in some cases to crack the code without key cards. And we assume they have."

One of the compromised systems was the most widely used code machine of all, the KW-7, a fact recently confirmed to us by four past or present NSA officials. Although the KW-7 has been replaced, it was once the mainstay of crypto-communications for the entire government. It was also used to communicate with many of our NATO allies. In addition to the KW-7, two NSA officials said that the reliability of the Navy's older KWR-37, used for one-way, shore-to-ship "Fleet Broadcast" messages, has also been completely written off.

These two code machines were not compromised by the so-called "brute-force" method, which entails having supercomputers run through every possible keylist combination. Rather, the Soviets apparently had so much material—including the KW-7 hardware, keylists and plain-text versions of messages sent on the system—that they were able to exploit "design flaws" in the KW-7's logic that allowed them to do what the NSA had once believed impossible—"break" the machine's code formula without use of the daily keylist.

"The Soviets have always been reputed to be rather good in code breaking," says David Kahn, author of "The Codebreakers." "It's known that three things seem to be associated with success in code-breaking: musicianship, chess and mathematics. What are the three things the Russians are best at?"

Collectively, Walker and Whitworth supplied some six virtually continuous years of keylists for the KW-7 and KWR-37. Walker says he also provided the Soviets the technical manuals, complete with the precise schematics of the design logic, for the KW-7 and the KWR-37 systems. All subsequent KW-7 and KWR-37 equipment modifications were provided by Whitworth, both spies now confirm.

The Soviets had also obtained actual working versions of these machines. The United States lost both KW-7 and KWR-37 machines in January 1968, when North Korean gunboats seized the U.S. spy ship USS Pueblo for allegedly violating their territorial waters, and at least one other KW-7 was lost in Vietnam in the early 1970s, according to court testimony and Navy documents. So the "design logic" was unquestionably compromised, even when later modified.

The NSA's position at the time, according to former communications security chief Clark, was that even with one of the seized KW-7s, the Soviets "wouldn't be able to decrypt it unless they had a correct key." But within weeks after the Pueblo was seized, the KGB's codebreaking Department 16 had the KW-7's worldwide keylists, courtesy of their newly recruited spy, Warrant Officer John Walker.

While the Soviets never told Walker how successful their U.S. codebreaking efforts had been, they did once tell him when their KWR-37 replica machine had stopped reading secret U.S. messages in early 1980. Walker and Whitworth subsequently decided the problem stemmed from a new security device called a "Card Reader Insert Board," into which a keylist was placed and then reattached to the machine. Whitworth then sketched this new board and sent it on to Walker.

"I provided a diagram, a tracing . . . of the card reader," Whitworth admits when pressed. "That's true." The Soviets had no further complaints about reading the KWR-37 Fleet Broadcast messages.

By early 1984, the KGB's wish-list for Walker was narrowing. During a chilly meeting outside a Vienna mens' shop, Walker's KGB handler told him they still wanted "7 subsystems" (KW-7 hardware modifications), as well as naval operational orders and plans.

And, in a request that once again seemed to demonstrate the Soviets still had better access to U.S. secrets than either Walker or Whitworth, the KGB agent asked for copies of something called an "NCM," which Walker says stood for some sort of "crypto-related 'National Command Memorandum.'" Neither Walker nor Whitworth had ever heard of this item before.

Fortunately, Walker and Whitworth did not have NSA "crypto clearances," and therefore never had access to the so-called "Blue Channel," used for super-sensitive "special intelligence" information. The Navy employs an entirely separate communications system on ships and bases for such messages, although the systems did use some of the same equipment, including the KW-7 and the KWR-37.

The severe damage done by the Walker ring probably ended several years before they were caught. In the early 1980s, the NSA introduced various safeguards, including canister-type keylist dispensers, that prevented someone from removing a keylist and later returning it; "limited" technical manuals, which contained no logic diagrams; and unphotographable types of keylists for the Navy's new, advanced code machines.

Walker now says the creators of those inovations "should be awarded medals."

But the demise of the Walker ring didn't stop the KGB. At about the same time Walker's crypto supply to the Soviets ended, Army Warrant Officer James Hall

had just come on line in Berlin. As a signals-intelligence specialist for the NSA's military subsidiary, the Army Security Agency, Hall had access to a broad array of U.S. crypto systems, including the KW-7, according to sources. U.S. sources say that Hall has apparently admitted supplying "important signal-intelligence information" to the KGB's proxies in East Germany from late 1982 to early 1988. Hall is now said to be cooperating with authorities.

What's ominous is that early last year, Hall apparently was told by his Soviet controllers "to cool off his activities." "Hall was flushed," concludes one intelligence source. "There's still someone else out there."

The likelihood that the codebreakers of the KGB's Department 16 were "not only able to copy, but were able to solve" U.S. codes, deeply worries Kean College mathematics professor Cipher Deavours, long close to the secret world of codes and the editor of Cryptologia. "The main assumptions under which the National Security Agency [operates] is that even if the enemy has possession of the machine, he won't be able to read any traffic without the key. That assumption was wrong. And our entire crypto-design philosophy is built on that."

"You have to assume they're certainly not arresting everybody," says Walker, from his cell in the isolation block of the most secure federal prison at Marion, Ill. "There are obviously other spy rings out there and other players. The fact that there were cryptographic systems and other types of systems that they didn't want is clearly evidence that they had other sources."