From George Mason University's

History News Network

WWW.HNN.US

When you are finished with the comments for this entry, close the window to return to "History Being Talked About Archives 12-10-03 to 12-28-03".

KW-7 Key Lists (#1770)
by Jim Williams on July 25, 2002 at 11:55 AM
Not only am I a history professor. I also was an Army Signal officer in the Vietnam era who worked some with generally low-level codes, including KW-7 keylists. This essay reveals a lack of understanding of cryptography and underestimates the careful complexity of our cryptographic system. If this is the level of care which Lerner put into the rest of his book, then the book is not credible.

The Soviets' possession of the operating manual for the KW-7 and the machine itself were not disastrous compromises, nor were even the seizure of the keylists on board the U.S.S. Pueblo. There was not one universal KW-7 keylist. There were hundreds, probably thousands (my vague memory is that my index of keylists was updated bi-monthly or quarterly and was hundreds of pages long, with 30-50 codes listed per page; this may have been only the Army's codes also), with different missions and organizations having different keylists. Moreover, each specific list was good for only one day, sometimes for even shorter periods (3 hours, 6 hours, etc.). How many days of keylists did the Pueblo have? I'm not a Navy guy, but I bet it wasn't more than a month's worth at a time - and probably for a few radio nets not directly related to Vietnam. The NSA and DoD intelligence and communications personnel resist whenever possible the excessively broad use of a single key to reduce the possibility of it being compromised and the damage caused if it is compromised. In other words, they aren't dumb, despite the cliche that military intelligence is an oxymoron.

NSA knew and knows exactly who has which editions of which keylists. The NSA and DoD intelligence agencies should have and probably did immediately supersede all keylists known to have been on the Pueblo. However, that information is probably classified.

Walker's cryptographic treason was more serious, since he may have gained access to global, strategic codes, not merely naval operational intelligence codes. I don't know which codes he betrayed to the Russians, but do not underestimate the difficulty of betraying a whole lot of codes on an ongoing basis. A lot of paper is involved, and copying thousands of pages a month invited detection and arrest, while people would notice if the actual serial number accountable keylists were missing.

More dangerous than the seizure of keylists in the Pueblo, keylists which probably had a limited application, would have become obsolete quickly and were probably immediately superseded, was the possibility that the Russians, by analyzing the sequence of the characters in the keylist, could figure out the computer program which generated that specific group of keylists. That's why we had to destroy used or obsolete unused key lists carefully and thoroughly. Did the Soviets figure the computer program(s) out? Maybe the NSA or CIA knows. I sure don't - no "need to know". However, to do this required luck, great ingenuity and great computers. The Soviets had the ingenuity, but did they have the luck and the computers? Maybe some day we'll find out. If they did, however, it is a little surprising that we have not yet heard about it.

[Reply] [Return to Comments]

RE: KW-7 Key Lists (#1791)
by Brian Gordon on July 26, 2002 at 11:55 PM
I was a shipboard naval officer in 1968 when the USS Pueblo was captured. Among my duties was to serve as what the Navy called a Registered Publications Custodian, meaning that I kept custody of all the crypto codes for the ship (my office was a walk-in safe). The usual practice was to carry several months' worth of key cards for the various crypto machines, and my job was to keep inventory of them, dole them out to the communications people as needed, and to shred and burn old codes. When the Pueblo was captured, it appeared

that no one was absolutely certain what codes it had on board, and the result was a slew of messages to the effect that yet another series of codes was assumed to have been compromised, and that therefore it was necessary to destroy another month's worth of key cards. Once we reached port, we had to stock up on new codes. The line at the door of the Honolulu NSA distribution point was almost as long as the line of burn-bag-toting RPCs at the Pearl Harbor naval base's incinerator. (Most ships had shredding capability, but incineration usually required a shore facility.) What amazed me at the time (assuming, of course, that the destruct orders were based on actual inventory carried aboard USS Pueblo) was how many seemingly irrelevant code series had been carried on board that ill-fated snoop-ship. I recall seeing NATO operational key codes included on the shred-and-burn lists that came out following Pueblo's capture. It would have been more sensible to have such a vessel going in harm's way carry only a minimum inventory of codes, not the standard worlwide inventory issued to other ships. (And contrary to Professor Williams's thread above, Navy ships, including, apparently, USS Pueblo, carried several months' worth of keylists, not just enough for one month, so when it became evident that USS Pueblo had been captured with its crypto gear and code inventory mostly intact, every ship in the fleet went through several months' worth of codes in less than a week. We would switch to a series for the following month, then the next day a message would come through saying that that series was also assumed to have been lost, and ordering a switch to still another month, and so on.)

Of course, it could also be argued that, despite security breaches, spies like the Walkers, incidents like the capture of the Pueblo, inadvertent leaks of classified information, and so on through a dismal list of intelligence mishaps, none of it made much difference----even if the Soviets were reading our mail, they STILL lost the Cold War! They even had the technical manuals for the 1980s KH-11 spy satellite, and they still couldn't reverse-engineer anything close to it.

[Reply] [Return to Comments]

RE: KW-7 Key Lists (#4849)
by John G Linton on November 15, 2002 at 3:10 PM
I found your comment about KW-7 key lists interesting. The public has been interested in the subject after the televised airing of "The falcon and the snowman." and other television movies about the Walker navy family, and most currently, the FBI agent who sold information. I think the public simply gets lost in the technical details of the televised presentations, and becomes disinterested in the subject. There also appears to be some public confusion between fiction and reality. I simply regard the world of cryptography as a means of communication, not a black world of Dr Stranglove. I see much of the public fear as unwarranted.

I was a repair SP-5 during the vietnam era and worked for two years on the repair and upgrade of field returns. I would trouble shoot and repair returns to the component level. I have
seen the inter-net posted image of the KW-7 ORESTES posted by ontario and I can certify the images and your comments are true and accurate.

I hope someday to author letters that may be of interest to people in the field of communications and communications history.