Volume 35 Number 4 *July-August*

Article 4

1982

Soviet Radio Electronic Combat and the US Navy

Guy Thomas *U.S. Navy*

Follow this and additional works at: https://digital-commons.usnwc.edu/nwc-review

Recommended Citation

Thomas, Guy (1982) "Soviet Radio Electronic Combat and the US Navy," Naval War College Review: Vol. 35: No. 4, Article 4. Available at: https://digital-commons.usnwc.edu/nwc-review/vol35/iss4/4

This Article is brought to you for free and open access by the Journals at U.S. Naval War College Digital Commons. It has been accepted for inclusion in Naval War College Review by an authorized editor of U.S. Naval War College Digital Commons. For more information, please contact repository.inquiries@usnwc.edu.

Soviet Radio Electronic Combat and the US Navy

Lieutenant Commander Guy Thomas, US Navy

he battle for control of the electromagnetic spectrum will be the most important battle of any war with the Soviet Union. If we lose that battle then all else is lost as well. In fact, according to Admiral Gorshkov "the range of electronic detection and reconnaissance can control modern warfare."

The United States is only now becoming aware of that fact while the Soviets appear to have fully recognized the importance of Electronic Warfare (EW) and the potential benefits of Command, Control, and Communications Counter Measures (C³CM) for some time.² They have incorporated their ideas into a concept they call "Radio Electronic Combat" (REC). From a number of sources it is apparent that the Soviets believe that REC will be very important in any future war.3 Open source literature indicates they are working very hard in both the theoretical and applied scientific fields to solve the problems of REC.4

It is known that they have a standard doctrine controlling REC in all branches of their armed forces.⁵ Given the Soviet bent on centralized organization there may well be a single REC organization similar to the other "Special Troops." If there is a single REC organization, its authority must come directly from the General Staff, but it is not clear if direct liaison between the different branches would be authorized.6

The current edition of Sovetskaya Voyennaya Ensiklopediya (Soviet Military Encyclopedia) defines "radioelectronnaya bor'ba" (Radio Electronic Combat/REC) as follows: "Radioelectronic combat is the set of measures performed for reconnaissance of the electronic material and systems of the enemy and their subsequent electronic neutralization, as well as the measures performed for the electronic protection of friendly electronic material and systems. Radioelectronic combat measures are carried out in conjunction with the destruction of electronic material, principally by weapons that home on emissions."7

REC is part of a larger doctrine called Maskirovka. Maskirovka also includes such actions as visual camouflage, operational security (OpSec), terrain masking, dummy aircraft and installations, and disinformation, but this paper will discuss only REC, the electronic portion of the Maskirovka doctrine.8

Soviet doctrine is not just to deter war but to be able to fight to win if war does break out. This is as true in REC as anywhere else. They have invested large sums Published by U.S. Naval War College Digital Commons, 1982

1

ensuring that they can, at the very least, deny our use of the electromagnetic spectrum and can exploit or manipulate those emissions which are not either jammed or destroyed.9

REC can be divided into four divisions:

- 1. Exploitation
- 2. Deception
- 3. Denial
- 4. Destruction

Major General Doyle Larson, Commanding General of the Joint Electronic Warfare Center, a man deeply involved with coordinating US Air Force C³CM strategy, has called those four divisions "The Four Horsemen of the Apocalypse of Modern Warfare." Almost certainly it will be apocalyptic for any nation that cannot overcome them in the modern battlefield, be it on land, at sea, in the air or in space. Recently excellent articles have been published dealing with REC as it pertains to the Army and the Air Force. However, while the Navy obviously recognizes various parts of the threat and there are multiple references to different aspects of REC as it pertains to the Navy, extensive research has failed to uncover any single writing dealing with all aspects of the problem. Beyond doubt, more discussion within the Navy is needed. This essay will collate various unclassified references in an attempt to provide a clear picture of the threat to the Navy from REC.

The Soviet Navy is believed to have an integrated intercept and jamming capability which includes dedicated active jammers, deceptive devices, chaff, and possible decoys. 10 It is not clear if there is a plan for the employment of REC by a mixture of platforms. The major drawback to such coordination would be the need for sophisticated tactical communications.

Given the very structured, doctrinaire method of control of Soviet forces, it is highly likely that plans for such coordinated operations exist but are not exercised due to security considerations. There may well exist plans across service lines, with the various Soviet Air Force organizations scheduled to assist the Soviet Navy in attacking US Navy elements with electronic as well as other means. Admiral Gorshkov seems very proud of the coordination his navy has with the other services, especially long-range aviation. There is no doubt that in a war with the Soviet Union, the assets of every service would be targeted against any force threatening Soviet forces, especially those located near the "Homeland." While we look on C³CM as a potent "force multiplier," the Soviets look on REC as a primary weapon. 12

Let us examine in turn each of the four divisions of REC to see what the Soviets are capable of and what assets they can bring to bear on our Navy.

The first horseman of the REC apocalypse is Exploitation. Exploitation is the passive use of the other side's emissions for one's own good, i.e., electronic warfare support measures (ESM) or signals intelligence (Sigint). The only difference between the two terms is that "passive electronic warfare type systems that have direct input to the fighting commander in real time or near real time, we consider to be ESM," while Sigint has no direct combat applications.

ESM is the cornerstone of EW/REC/C³CM. It provides locational data, both in reference to where a signal is located in the electromagnetic spectrum and in geographical terms. It also provides a good indication of enemy intentions to the

The Soviet Sigint threat to the US Navy has been recognized for some time. What it not so widely recognized is that the Soviets plan to use Sigint as ESM for real time targeting for all three of the other REC capabilities. ¹⁴ It is clear from numerous sources that the Soviets have an immense effort underway to exploit our communications, radars, data links and telemetry transmissions. ¹⁵ That exploitation effort provides intelligence in peacetime, but it would provide targeting in time of war.

The Soviets have sensors in every environment: land, sea, air and space. In that perhaps the greatest REC threat to the US Navy battle group is presented by the Soviets' specialized ESM/ECM aircraft, we will discuss them first.

All Soviet Naval Aviation (SNA) reconnaissance aircraft are postulated to have at least an electronic (Elint) capability. Many may well have a communications intelligence (Comint) including radio direction finding (RDF) capabilities as well.¹⁶ In fact, it is this writer's suspicion that all aircraft of the same designation do not have exactly the same sensors on board, e.g., not all TU-95 Bear Ds have exactly the same sensor suites as every other Bear D. Given airframe loading and lift capability as limiting factors, as they most definitely are, the Soviets may have intentionally chosen to fit some sensors in one airframe and others in another, without changing the basic outward configuration of that class of airplane for operational security reasons. The reason for going to two airframes would be to give them more REC capability. The Soviets may well have planned from the beginning to have the two different sensor suites fly as a complementary pair. Although it is generally believed that the reason for at least two Soviet reconnaissance aircraft being on every mission is to permit them a wide variety of approach altitudes and patterns as well as safety considerations, the above speculation could also be valid. It is suggested that the inner configuration of any two SNA aircraft engaged in any surveillance operation could be different. This is not to say that every sensor station is different, but rather that while the two aircraft have a great deal in common (50 percent or so), they also have a number of sensors unique to one aircraft or the other. This would allow the Soviets the luxury of not having to find room inside an already crowded airplane for every single piece of electronic warfare/reconnaissance gear they need for any single mission. This would also mean that every flight of two Soviet reconnaissance aircraft would actually be more than two times more capable than a single aircraft, they would be synergistic.

Even if they are not synergistic, the Soviets have a large number of aircraft configured for some form of Elint or Comint collection. SNA aircraft believed to have an Elint or Comint or both capabilities include: about 50 TU-95 Bear Ds "well equipped with ECM." Airframe size (very large) indicates that Bear Ds could also have several Comint positions as well as Elint and DF capabilities. Bear Es flown hy long-range aviation and Bear Fs flown by the SNA may also have a Sigint capability; about 50 TU-16 Badger D/E/F/H/J/K aircraft with at least an Elint capability, 22 TU-22 Blinder Cs with an Elint system and 8 AN-12 Cub Bs, a large transport similar to a C-130, but extensively modified to be a Sigint aircraft with an estimated capability to intercept and DF radio, radar and data link transmissions. Both the SNA and the Red Air Force also fly another variation of the AN-12, Cub C, a very comprehensive jamming platform, but that will be discussed later in this paper.

Another aircraft that routinely operates over water is the Soviet Air Force subordinated IL-20 Coot A. It is believed to have both a Comint and Elint collection Published by U.S. Naval War College Digital Commons, 1982

capability, and it is also postulated to possess a very sophisticated side-looking radar.²⁰ The Soviet Air Force also has several classes of shorter range aircraft that could collect against a wide variety of emitters albeit at a substantially closer range to the shore. Those aircraft include: the MIG-25 Foxbat B/D, which may have internally mounted Elint collection and DF systems,²¹ as well as a SLAR capability. The Yak-28 Brewer D and the Fishbed H are both reported to have a reconnaissance pod with an Elint capability.²² The SU-20 Fitter H is also equipped with a centerline reconnaissance pod which is postulated to have an Elint DF capability.²³

Additionally, the Red army operates helicopters with electronic warfare missions²⁴ thus there is no technical reason why a Sigint capability could not be fitted to the SNA's KA-25 Hormone B helicopters, currently flown from many Soviet cruisers as well as Moskva and Kiev-class air-capable ships as part of the ship's over-the-horizon fire control sensor suites.²⁵ Hormone Bs may well already have a rudimentary Elint DF capability. By putting ESM sensors on board a helicopter, the Soviets would substantially increase the passive detection range of their fleet. An Elint operator can tell when a detected (intercepted) signal is strong enough to counter-detect his platform. By staying below the detection horizon of the exploited emitter, an airborne operator can remain undetected while maneuvering to acquire and then refine a Sigint derived fix. A helicopter would be one way to provide that type of information far at sea without using land-based air. The large, more air-capable ships such as Kiev and Moskva, would be the logical choices for helos with a Sigint capability. They could carry one or two Sigint helos as well as their regular ASW/OTH helos.

Another way to solve the passive target acquisition problem is with Sigint satellites. It is highly probable that, as technology is refined, space sensors will someday in the not too distant future supplant aircraft as the greatest threat to a carrier battle group. As of this time, spring 1982, the Soviets are credited with having developed several different types of Elint satellites. Many of their satellites are presumed to be targeted against US Navy emitters, to have a DF capability and to be capable of downlinking their information in real time to Soviet command centers and weapons platforms. ²⁶ Thus, satellites can be used for cuing other sensors or targeting of either "hard" (bombs and missiles) or "soft" kill (chaff and jamming) weapons. In fact, "soft kill" weapons might be preferable in many instances because the Soviets just have to know the general area of their opponent to employ many REC weapons.

It appears that an important part of the combat capability of Soviet surface ships, particularly in AAW and ASMD, are the electronic warfare systems. Unclassified photographs indicate the Soviets place a great deal of emphasis in this area, back fitting the latest equipment into already operational ships. Since the Soviets are firm believers in "Better is the enemy of good enough," the back fitting of new equipment to replace equipment that is still in terms of service life, quite young, is almost unheard of in the Soviet armed forces. The routine back fitting of the latest in electronic warfare equipment is a very strong indication of exactly how much importance they place on EW. Along these same lines it is highly probable that most, if not all, Soviet major combatants are equipped with intercept equipment with especially trained personnel assigned to conduct Sigint collection.

The Soviet Navy has over 50 ships of ten different classes configured specifically as intelligence collectors (AGI). Many of these ships are adaptations or conversions of https://digital-commons.usnwc.edu/nwc-review/vol35/iss4/4

trawlers, whalers, or survey ships, although there is a growing tendency to build intelligence collectors from the keel up as evidenced by the Primorye and Balzam classes. Until recently AGIs did not look particularly military. Some flew the Soviet naval ensign while others flew the ensign of the hydrographic organization. None were painted Soviet Navy grey or carried armament. Now, AGIs are clearly being given military identities with minimal AAW capabilities and a military paint and hull number scheme.27

This change of identity may, in part, be due to a perceived need to protect the AGIs within the mantle of the Soviet Navy. The Soviets obviously plan to use the ships in a hostile situation for as long as they are viable. By clearly identifying them as ships of the Soviet Navy, the Soviets may also hope to avert a Pueblo or Liberty type situation (although both of those ships were clearly marked as US Navy ships). Whatever the reason for this redesignation, the Soviets have a large number of ships capable of collecting Sigint and rapidly reporting it to central authority.28

Another capability that cannot be ignored is the civilian fleet; the merchant, scientific and fishing ships of the Soviet state. Many Soviet flag civilian vessels have been observed with HF/VHF/UHF direction finding antennas. This is considered a significant phenomenon, in fact the use of a civilian vessel to specifically monitor a US task force is not without precedent. It is believed that these ships routinely provide locational data on US naval units. At the outbreak of war these units would need to be put out of business, but by then, an aircraft carrier battle group may already be doomed by the ESM information provided by civilian manned ships.²⁹

Soviet submarines may also have a Sigint capability. There have been repeated reports of Soviet "spy submarines" in Swedish, Norwegian, and British waters since at least 1972.30 It is only reasonable to assume they can monitor communications and other electronic emissions as well. Thus there is the possibility of a submarine serving as an intelligence collector in much the same manner as an AGI. One of the major advantages of using a submarine in that role is that the target being collected against will probably not have any idea that he is within the range of someone who could exploit/monitor his transmissions and might not be as security conscious. Unclassified photographs of Soviet submarines seem to indicate that they have antenna systems that would support tactical Comint and Elint collection.

The Soviets are known to have land-based HFDF.31 Given the widespread use of HF in US Navy communications (NTDS, HiCoM, Orestes, etc.) HFDF is a distinct threat; at least against a battle group not in HF Emcon. The Soviet HFDF system may well be used to cue all other assets of the system—air, surface, subsurface, land and space.

This brings us to the second horseman of the C³CM apocalypse—Denial or Jamming. Admiral Gorshkov mentions jamming several times in his writings. He seems to be referring to ESM as well when he wrote "The maneuver will be carried out on the basis of data received from various electronic systems, even under the conditions of the most intensive electronic warfare, which, when correctly organized, can fully paralyze data acquisition and monitoring systems."32 There are two basic types of jamming: active, using electronic means to disrupt or deceive a signal (of whatever type: communications, radar, telemetry); and passive, using some form of material (metallic strips/aerosol) to disrupt a signal. Every type of jammers, such as IFF Spoofers.³³ The later type of jammer wil be discussed under Deception.

Once again the widest variety of platforms is found in the air. Many Soviet bombers, including several models of the TU-16 Badger, the TU-22M Backfire, the YAK-28 Brewer E and the TU-22 Blinder C, have been either designed or modified to carry a wide range of jammers of all types, both active and passive. Some of the systems are designed for protection of a strike force and installed in an aircraft dedicated to that mission while others are installed for self-protection on weapons-carrying platforms.³⁴ Additionally the Soviets have modified some of their AN-12 large transports to the "Cub C" configuration, which appears to be a most extensively equipped ECM platform.³⁵

Soviet Navy surface ships may also possess a wide range of jamming capabilities, including noise, deception, chaff and radar decoys. However, an in-depth assessment of Soviet shipboard jamming systems and tactics is precluded by the scarcity of open source information pertaining to the subject.

As with submarines in a Sigint role, very little is known about Soviet submarine jamming and deception capabilities. However, the Soviets have modified some of their Golf-class submarines with what appears to be an extensive communications outfit. 36 It is possible that those submarines may have a REC mission in addition to, if not in place of, their postulated C3 function. What could be more perfect than a jamming/deception platform that you would probably not detect until it started transmitting? Even then, given the confusion that even a partially successful IFF spoofing, pulse jamming, deceptive repeating or intrusion incident generates, the submarine would probably remain undetected, especially if the source could not be seen on radar. While radars can detect periscopes and a submarine would have to broach its antennas as well as its periscope to operate, ESM receivers on board the submarine would provide warning of hostile radars before they came within detection range. The Soviets have not hesitated in the past to place active emitters on board their submarines, even ones that required the submarine to surface to use them. Examples include the Whiskey Canvas Bag radar picket submarine and the Juliett and Echo II surface-to-surface missile-firing submarines. The idea of a submarine in an active REC role should not be ruled out.

The Soviets also have HF jamming stations ashore. "Strategic fixed jammers have been emplaced throughout the Soviet Union and ground forces have been equipped with mobile jammers, as well as specialized ESM vehicles." Those stations would, almost surely, be targeted against US Navy long haul communications, among other emitters. One of their principal targets might well be NTDS' Link 11 and Link 14.

The mobile system more readily lend themselves to missions such as IFF spoofing, meaconing (the overriding of Navaids to produce false bearing and range indications to deceive aircrews into following such indications) and intrusion which brings us to the third horseman of the electromagnetic apocalypse—Deception. Again, we know very little about Soviet capabilities but it would be wise to assume that they do have each of those capabilities on aircraft, surface combatants and submarines as well as auxiliaries, especially their AGIs. ³⁸ Incidents have been reported wherein Soviet units, both air and surface, have been either the only possible source or the most likely source of an incident involving either jamming or deception. About all that we know about deception is that the Soviets continue to give very high priority to it

Thus we come to the fourth horseman—the hard kill, Destruction. This is accomplished with every weapon in the inventory: guns, bombs, rockets, torpedoes or missiles. It is probable the Soviets have given some thought as to which targets are best attacked by weapons, which by jamming, which to deceive and which to exploit. "Soviet EW specialists, whose skills and equipment currently exceed our own to a significant extent, seek soft kills against a comprehensive spectrum of targets: command/control and communications, radars, fire control systems, infrared and optical seekers, navigation aids, and so on."40 The ordering of the physical destruction of an emitter is obviously carried out by someone in operational control; however, the locating data on the "hostile" emitter comes from the Soviet EW specialist who is part of the REC system. He may well have the responsibility of recommending whether the emitter should be taken under attack or not. That destruction might come from an antiradiation missile carried by a bomber or submarine, a standard active seeker type missile fired from above, on or under the sea or the destruction may come via more traditional means, such as a torpedo, bomb or shell. The one thing in common with each of the above is that the location was ascertained by REC.

One other aspect of REC should be explored and that is the threat to our own C³I facilities. If you take as a given that we are going to go to great lengths to protect our seaborne and airborne C³I assets as that is part of the nature of war, then the only thing left to discuss is whether we plan to adequately defend our shore-based C³I facilities. Sites that fall into the above category include, but are not limited to: Sosus stations, communications facilities, HFDF sites, remote sensor downlink sites and radar stations. The location of many of these sites dictates their vulnerability. Many of them have common characteristics. First, they are all fixed sites. Second, their exact location is known to anyone who wants to know. Third, they are often near the sea. Fourth, rhey are often lightly defended. Fifth, they are often isolated.

From the above list, several vulnerabilities suggest themselves. Sabotage by either "unfriendly natives" or small landing teams is a distinct possibility. Saboteurs would not necessarily have to attack the site itself. It might be enough for a team to knock out a station by cutting the cables to the power supply or destroying its microwave links. Air strikes are another possibility, but obviously only for those stations within range of Soviet air. However, places like Misawa, Japan, and Sinop, Turkey, are well within range as are many other places in Europe, Japan, and Korea. Submarine-launched cruise missiles, possibly fitted with a persistent CB agent are a third possibility. It should not be outside Soviet technology to develop a very effective chemical warhead for a missile of the size of an SS-N-3.

The above is getting pretty far afield from what the United States usually thinks of the sterile world of EW and C³CM but it is all part of REC. The threat is real. The Soviets, with their REC systems, appear to have their act together. Only Clausewitz' "friction in war," actual combat, would reveal if appearances are deceiving and by then, it may well be too late to do anything about it. We seem to know a good deal about the bits and pieces of the problem. Let's hope that somewhere, somebody is doing something about countering it. In the meantime, we need to ensure that the Navy as a whole, down to every individual operating each single piece of electronic gear, is aware of exactly how vulnerable the Navy is

As Admiral Thomas Moorer, then Chairman of the Joint Chiefs of Staff said: "If there was a World War III, the winner would be the side that can best control and manage the electro-magnetic spectrum."41

NOTES

- Robert B. Bathurst, Understanding the Soviet Navy: A Handbook (Newport, R.I.: Naval War College Press, 1979), p. 127.
 - 2. John M, Collins, U.S. Soviet Military Balance 1960-1980 (New York: McGraw-Hill, 1980), p. 329.
 - 3. Roger Villar, "Denying Tactical Information," Navy International, April 1980, p. 208.
- 4. Naval Intelligence Command, "Soviet Electronic Countermeasures," Soviet Naval Electronic Warfare, 15 May 1979, p. vii.
- 5. Scott James, "Maskirovka: Are the Russians Taking Us Down the Garden Path?" Defense Electronics, August 1980, p. 48; D.B. Lawrence, "Soviet Radio Electronic Combat," Air Force Magazine, March 1982, p. 88; "REC—An Integral Part of Soviet Doctrine," U.S. Army Aviation Digest, May 1980, p. 30; Norman Polmar, "Soviet C³," Air Force Magazine, June 1980, p. 64.
- Harriet Fast Scott and William F. Scott, The Armed Forces of the USSR (Boulder, Colo.: Westview Press, 1979), p. 244.
- 7. "Radioelectronnaya bor'ba," Sovetskaya Voyennaya Ensiklopediya (Moscow: Voyenizdat, 1979), v. 7, p. 29.
 - 8. James, p. 47; Lawrence, p. 91.
- 9. Paul H. Backus, "The Nature and Management of ECCM," Journal of Electronic Defense, November/December 1978, p. 25.
 - 10. Ibid.
 - 11. Bathurst, p. 135.
- 12. S.A. Vakin and L.N. Shustov, Principles of Jamming and Electronic Reconnaissance—Osnovy Radioprolivodeystviya I Radioteknicheskoy Razvedki (Moscow: Izd-vo Sovetskoye Radio, 1968), translated by Translation Division, Foreign Technology Division, Wright-Patterson AFB, Ohio, p. xv.
- 13. "An Exclusive Interview with Rusty Porter," Journal of Electronic Defense, November/December 1979, p. 26.
- 14. David T. Easter, in his article "ASW Strategy: Issues for the 80's," U.S. Naval Institute Proceedings, March 1980, provides an excellent thumbnail sketch of Soviet Sigint and reconnaissance capabilities: "The Soviet ocean surveillance system is composed of a wide variety of intelligence collectors, ranging in complexity from relatively simple high frequency direction finding facilities to highly sophisticated radar and electronic intelligence satellites. The SOSS correlates data collected from all types of sources, including merchant ships, naval combatants, aircraft, and satellites. Some components of the SOSS, such as the "Bear D" aircraft, provide targeting solutions and missile guidance functions for submarine-launched cruise missiles through sophisticated data link systems," p. 37. Lt. Easter also says "The most imminent breakthrough" in Soviet submarine anti-surface warfare capabilities is the provision of real-time external targeting data to patrolling submarines through sophisticated SOSS and command, control and communications networks," p. 35. He goes on to say "The SS-N-3 cruise missile launched by an 'Echo II' SSGN today, supported by 'Bear D' target fixing and mid-course guidance, will have been superseded by the SS-N-9 or SS-N-12 launched by 'Papa'—or 'Alfa'—class SSGNs and supported by satellite systems before the end of this decade," p. 38. It is not clear to this author if the SOSS is a part of the REC service or vice versa or whether SOSS is an invention of Western naval intelligence.
 - 15. Lawrence, p. 89.
 - 16. Ibid.
 - 17. Jean L. Couhat, Combat Fleets of the World (Annapolis: Naval Institute 1977), p. 539.
 - 18. Lawrence.
 - 19. Ibid.
 - 20. James, p. 48.
 - 21. Lawrence.
 - 22. John W.R. Taylor, "Gallery of Soviet Aerospace Weapons," Air Force Magazine, March 1982, p. 102.
 - 23. Ibid.
 - 24. Ibid.
- 25. Office of the Chief of Naval Operations, Understanding Soviet Naval Developments (Washington: U.S. Govt. Print, Off., 1981), p. 128. (Hereafter referred to as "Understanding ")
- 26. Norman Friedman, "C3 War at Sea," U.S. Naval Institute Proceedings, May 1977, p. 135; fournal of Electronic Defense, July/August 1980; Easter, p. 38.

27. "Understanding ," p. 46. https://digital-commons.usnwc.edu/nwc-review/vol35/iss4/4

- 28. Richard Deacon, The Silent War (New York: Hippocrene Books, 1978), p. 227.
- 29. "Understanding ," p. 63.
- 30. Deacon, p. 233.
- 31. Lawrence, p. 89.
- 32. S.G. Gorshkov, *The Sea Power of the State* (Oxford, England: Pergamon, 1979), p. 208, translated from Morskaya Noschch Gosudarstva (Moscow: Voennoe Isdatel'stvo Ministerstvo Oborony, 2nd Revised edition, 1976).
 - 33. Vakin and Shustov, p. xii.
 - 34 Villar, p. 32.
 - 35. James, p. 186.
 - 36. "Understanding . . . ," p. 91
 - 37. "International Report," Journal of Electronic Defense, February 1982, p. 21.
 - 38. Vakin and Shustov, p. xiii.
- 39. Evan P. Rolek and Michael Tutin, "Silent Sensors & Human Operators-Hidden Threats," Journal of Electronic Defense, February 1982, p. 55.
 - 40. Collins, p 233.
- 41. A sign next to the door of the Director, Joint Electronic Warfare Center, Kelly Air Force Base, Texas.

Lt. Cdr. Thomas, a Naval Security Group officer, has been ordered to the staff of the Naval War College after a year as a student.



