Naval War College Review

Volume 47
Number 1 *Winter*

Article 11

1994

I. Signals and Sealift: Merchant Ship Communications Security

Eric R. Bodner

SET AND DRIFT

— I —

Signals and Sealift
Merchant Ship Communications Security

Lieutenant Eric R. Bodner, U.S. Naval Reserve

THE U.S. MERCHANT MARINE HAS RECENTLY enjoyed a great deal of attention, and rightfully so. Sealift played an important role in our success in Southwest Asia. The spotlight on shipping has revived awareness of the merchant marine's defense role and of our dwindling sealift capability. But there is another aspect of the merchant marine that needs to be brought to light: shipping's vulnerability to electronic warfare. The communications systems used to direct strategic sealift can be exploited. The signals of our merchant ships are open to hostile interception, exploitation, and disruption. That state of affairs can and should be corrected, lest we suffer needless losses in the future.

During the Gulf War a favorable set of circumstances allowed us to transport cargo without enemy interdiction. We should be thankful that, this time, the threat to Allied shipping was deterred, and thus nearly nonexistent. In a future conflict our adversary might be capable of using the electromagnetic spectrum to our disadvantage. Since most merchant vessel communications are unprotected against hostile direction-finding, intelligence gathering, imitative deception, and jamming, we may discover that an enemy is able to employ our communications as a weapon against us and disrupt the flow of logistics by sea.

To ensure that the afterglow of recent success has not dulled our senses, we should remind ourselves that merchant ships are targets. During the Iran-Iraq

Lieutenant Bodner is a member of the Merchant Marine Individual Ready Reserve Group, U.S. Naval Reserve. He is employed as a civilian ship's Radio/Electronics Officer on vessels under the operational control of the Military Sealift Command.

war, several hundred vessels were set upon with rockets, bombs, and missiles.[1] During the Falklands War, British and Argentine merchant vessels were sunk.[2] During the Second World War thousands of ships went down, and the casualty rate for American civilian sailors was exceeded by that of only one branch of the U.S. military, the Marine Corps. Although another Battle of the Atlantic is unlikely, the submarine, anti-shipping weapon *par excellence*, still remains a threat: "It could prove disastrous . . . to assume, in a future Third World crisis to which U.S. forces have been committed, that the absence of Soviet involvement had virtually eliminated the underwater threat from submarines."[3] It seems that a variety of threats to shipping yet remains in the post–Cold War, post–Gulf War era.

The Electronic Battleground

Granted, merchant ships can be expected to go into harm's way. But why are the communications signals of merchant vessels so vulnerable? For that matter, why are signals so important? Signals have been not only important but decisive in some contexts, as they were in a particular series of events that occurred in 1942. During a convoy operation in that year, the escort vessel *Spikenard*, a Canadian Flower-class corvette, was sunk by a U-boat, which then succeeded in imitating the *Spikenard*'s radio communications and learned thereby where the remainder of the convoy was headed. As a result, the U-boat was able to intercept and again attack the convoy. In another instance, a freighter was diverted back to port by, evidently, a U-boat imitating a naval communications station.[4] Many times in 1942 the German submarines that inflicted such heavy losses on American shipping "derived great benefit from American carelessness with radio."[5] One U-boat ace, Kapitanleutnant Hardegen, reported to Admiral Karl Dönitz that he found merchant ship radio traffic "the most important resource for successful operations."[6]

The cryptologic battles that altered the history of the Second World War have been detailed in a number of books and articles. One of them, *The Sigint Secrets*, suggests that what was actually more decisive than code-breaking was the refinement and application of the all-inclusive science of signals intelligence, including direction-finding and traffic analysis.[7] Don E. Gordon's *Electronic Warfare* supports the same premise: that cryptanalysis is but a subset of a larger set of electronic warfare (EW) tools.[8] That premise is an important one. It implies that encrypting a message is not enough—much can be gleaned from even an encrypted transmission. It suggests that those who need to communicate securely would be well advised not only to encrypt the meaning conveyed within a transmission but to conceal the transmission itself.

The policy today, because analysis and exploitation of electronic signals has become fundamental to the conduct of warfare, is to communicate with low

probability of intercept, for which a number of technical and procedural approaches (known as LPI techniques) are available and in use. The electromagnetic spectrum is as much a battleground as the land, the air, or the sea. Those who fail to grasp that concept put themselves at great risk. Just as every Marine is a rifleman and every sailor a damage-controlman, so every unit needs to be a communications security group. How does our merchant marine measure up?

Our Communications Capabilities

The radio gear carried by merchant ships today is suitable only for business-as-usual, peacetime purposes. Because our merchant marine lacks the equipment and procedures for communicating in any sort of EW environment, we may lose vessels and valuable cargos in the early days of some future contingency, as we did in World War II. In 1992 the same resource once exploited by U-boats is still available to potential enemies—our vessels' radio traffic—and our merchant ships remain vulnerable. The author's experience during Desert Storm is illustrative. A few days before the start of the ground war in February 1991, the freighter SS *Cape Catoche* was directed to proceed northbound through the Arabian Gulf. Carrying 5,000 tons of ammunition, we passed near mine danger areas and advanced so close to Kuwait that we could see the glow of burning oil wells and hear and feel the concussion from the shelling. We unloaded our cargo at al-Mishab, a port in the northernmost part of Saudi Arabia. Throughout the entire operation our only tactical link with the Navy, our short-range communications "lifeline," was that most public of international calling frequencies—VHF channel 16, the seagoing equivalent of Citizen's Band radio.

Merchant ships sent into harm's way ought to be capable of communicating by not only encrypting or scrambling the content of a transmission but also by concealing the transmission itself (which is the purpose of the LPI concept). There will be times when merchant ships will need a means of communicating rapidly and securely at radio line-of-sight distances, in an LPI mode.

Why has this need not been met? There are complications. The merchant marine is expected to function both in the commercial as well as the military sectors, and the communications requirements of the two roles are overlapped and somewhat in conflict. Because merchant ships engage in commercial pursuits most of the time, going to war only infrequently, the military requirements tend to be de-emphasized by the commercial operators and owners. The Navy also tends to downplay requirements for merchant ship communications, because after all, the merchant marine is not a part of the Navy; in fact, it is traditionally considered by the Navy to be a poor relation. Sealift lacks glamour; as a retired admiral of the Royal Navy has suggested, "There is a tendency in the Western armed forces to think that 'one

is not doing a man's job unless one is in a fleet destroyer, or flying an attack aircraft, or dashing about . . . in a main battle tank.'"[9]

Probably the most troublesome problem inhibiting secure communications for merchant vessels, however, is the tremendous overhead of accountability. Communications Security Material System accounts with "two-person integrity" are costly to maintain. Furthermore (as if cost were not enough of a problem), the mariners who work onboard commercial ships come and go according to pay, working conditions, benefits, and job availability (as in any commercial environment), a circumstance not conducive to control and accountability.

Improving Our Capabilities

There is no single all-encompassing remedy for the lack of secure communications for strategic sealift. However, there are at least two ways of approaching the problem: by adding on to merchant ships equipment and manpower from the Navy's existing communications systems, or by developing new systems. The first approach was used when U.S. Navy Armed Guard radio teams were embarked on some World War II merchant vessels, and again in the early 1980s when containerized communications suites were placed on vessels acquired from the United Kingdom by the Military Sealift Command.

The second approach, the development of new communications systems, undoubtedly has more promise. The new technology that may hold out most hope for correcting the merchant marine's tactical communications deficiencies can be found in the commercial telecommunications marketplace: digital radio techniques, specifically direct-sequence spread spectrum, now used in wireless computer local-area networks (LANs). Spread spectrum is an advanced modulation technique with an inherently low probability of intercept that has long been used by the military but seldom in the commercial sector for equivalent purposes. The basic idea is to "dilute" or broaden a radio transmission to cover a very wide band of frequencies. One cannot listen in on a spread-spectrum signal by tuning a conventional receiver to a specific spot on the dial; the spread-spectrum transmission is spread all across the dial. The signal remains undetectable, noticeable only as a slight increase in overall noise. A special receiver, programmed with a unique algorithm, is required to "de-spread" the signal and recover its intelligence.

Today one can buy a small UHF radio transceiver that connects to any desktop computer and transmits and receives a high-speed data stream (fast enough for digitized voice) for local-area networks via direct-sequence spread-spectrum modulation. Considering the sophistication of the technology, the unit price of a few hundred dollars is remarkably low. The circuitry at the heart of these

wireless LAN transceivers can probably be adapted to other spread-spectrum applications: it might be relatively inexpensive to design a line-of-sight voice radio for rapid tactical communications, using LPI and simple procedures for remote keying as used in the STU-III secure telephone (thereby alleviating the need for two-person accountability for communication security material).

There remains the question of long-range communications. During the Gulf conflict most allied merchant ship long-range communications needs were well served by the MARISAT satellite system. Its commercial voice and teletype circuits were reliable and effective; in the few cases where vessels were provided with the STU-III secure telephone, the circuits were even encrypted. The STU-III, which alleviates the administrative-security overhead, is a step in the right direction. The STU-III/MARISAT combination is a highly effective and simple solution, as far as it goes.

We were fortunate in 1990–91, however, that Iraq chose not to jam the MARISAT uplink frequencies. That task would probably be a trivial one for even a poorly equipped practitioner of electronic warfare. By jamming MARISAT uplink frequencies assigned for the Indian and eastern Atlantic oceans, a transmitter located in Iraq (or in any of dozens of other countries within the satellite's "footprint") could have blocked satellite communications for all merchant ships located east of Italy and west of Singapore. A third of the globe would have become a "black hole" for merchant ship communications. The command and control of strategic sealift would have ceased. What secure long-range circuit would ships have used if MARISAT had been jammed?

Perhaps merchant marine communications security requires the attention of experts from a variety of disciplines. Solutions might be found by drawing upon the technical knowledge of the Space and Naval Warfare Systems and naval cryptological communities, the realistic threat assessments of intelligence analysts, the tactical know-how of the surface warfare community, and the plans and practical experience of the Naval Control of Shipping Organization and Military Sealift Command. The collective knowledge of these specialists might be tied together by operations analysts, who could attempt to sort out every imaginable scenario involving merchant ships—in convoy or independent steaming, in an EW environment, with escorts either unavailable or available only in various states of readiness, and in situations short of war in which the need to avoid signals exploitation nonetheless exists.

For merchant ships that will require LPI communications, the most affordable and suitable solutions may be based on technology already available in the commercial sector. If no solutions are found, the ships and cargos of strategic sealift could be left vulnerable one day, and the men who serve on those ships would find themselves, as the Chinese proverb says, "living in interesting times."

Notes

1. Nigel Ling, "Merchantmen in the Gulf Front Line," *Jane's Naval Review 1985*, p. 62. See also Reginald Brown and Frederick Turner, "Passive ECM—Merchant Ships' Answer to Self Defense?" *Defense Science*, February 1985, p. 37; Shahram Chubin and Charles Tripp, *Iran and Iraq at War* (Westview, 1988), p. 277; and Edgar O'Balance, *The Gulf War* (Brassey's 1988), p. 216.
2. Andrew Ambrose, "Conflict and Commerce," *Jane's Naval Review 1982*, pp. 138, 143.
3. Desmond Wettern, "The Threat That Never Was," *Sea Power*, November 1991, p. 31.
4. Samuel E. Morison, *History of United States Naval Operations in World War II: Vol. I, The Battle of the Atlantic, September 1939 – May 1943* (Atlantic and Little, Brown, 1947), pp. 128–29.
5. D. van der Vat, *The Atlantic Campaign* (Harper & Row, 1988), p. 260.
6. Michael Gannon, *Operation Drumbeat* (HarperCollins, 1991), p. 405.
7. Nigel West, *The Sigint Secrets* (Quill, 1990), p. 27.
8. Don E. Gordon, *Electronic Warfare* (Pergamon, 1981), p. 4.
9. Desmond Wettern, "Wartime Adaptation of Merchant Ships," *Sea Power*, June 1983, p. 38.

Ψ

Annual Statement of Ownership

Statement of ownership, management, and circulation (required by 39 U.S.C. 3685) of the *Naval War College Review*, Publication Number 401390, published four times a year at 686 Cushing Road, Newport, R.I. 02841-1207, for 31 October 1993. General business offices of the publisher are located at the Naval War College, 686 Cushing Road, Newport, R.I. 02841-1207. Name and address of publisher is President, Naval War College, 686 Cushing Road, Newport, R.I. 02841-1207. Name and address of editor is Frank Uhlig, Jr., Code 32, Naval War College, 686 Cushing Road, Newport, R.I. 02841-1207. Name and address of managing editor is Pelham G. Boyer, Code 32A, Naval War College, Newport, R.I. 02841-1207. Owner is the Secretary of the Navy, Navy Department, Washington, D.C. 20350-1000. Average number of copies of each issue during the preceding 12 months is: (A) Total number of copies printed: 10,779; (B) Requested circulation, mail subscription: 6,481; (C) Total requested circulation: 6,481; (D) Free distribution by mail, carrier or other means: 4,060; (E) Total distribution: 10,541; (F) Copies not distributed (office use, left over, unaccounted, spoiled after printing): 238; (G) Total: 10,779. The actual number of copies of single issue published nearest to filing date is: (A) Total number of copies printed: 10,940; (B) Requested circulation, mail subscription: 6,733; (C) Total requested circulation: 6,733; (D) Free distribution by mail, carrier or other means: 3,972; (E) Total distribution: 10,705; (F) Copies not distributed (office use, left over, unaccounted, spoiled after printing): 235; (G) Total: 10,940. I certify that the statements made by me above are correct and complete.

(signed) Pelham G. Boyer, Managing Editor