Naval War College Review

Volume 47
Number 1 *Winter*

Article 10

1994

Set and Drift

The U.S. Naval War College

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

— II —
The Application of Space to Military and Naval Operations

Commander Thomas G. Seigel, U.S. Navy

EVERY OFFICER IS FAMILIAR WITH AT LEAST some aspects of the "Space Age," whether from our popular culture's fascination with space or from what space systems actually provide deployed forces on a daily basis with respect to weather, navigation, communications, and intelligence. What is probably missing from a professional officer's understanding of space, however, is a unifying concept, a strategic and operational-level understanding as to what space-based systems can and cannot provide in war.

To develop an organizing principle for the application of space to waging war, it would be useful to adapt the currently accepted mission of "sea control" to space. Thus, taking the definition of sea control as "the ability to use the sea where, when, and how desired," and applying it to the newest theater of military and naval operations, space, we may extrapolate to define "space control" as "the ability to use space where, when, and how desired in order to support or conduct military or naval operations."

There are two complementary functions, or roles, subsumed in this overarching concept of space control: "space use" and "space denial." Extrapolating again from naval terminology, these new terms have the following meanings: "space use" is the ability to employ space as desired to support or conduct one's own military or naval operations; "space denial" is the ability to prevent the enemy from using space to his own advantage.

With these concepts in mind, possible space use and denial functions can be enumerated easily. For *space use* there are currently seven.

- Combat
- Intelligence (including intelligence preparation of the battlefield, reconnaissance, and targeting)

Commander Seigel is a naval intelligence officer assigned to U.S. Space Command as chief of Space Support teams. He was previously responsible for Indications and Warning Intelligence Center watch operations for USSPACECOM and the North American Air Defense Command (NORAD). Previous duty included assignments as Intelligence Officer of the USS *Enterprise* (CVN 65) and to the Naval War College faculty.

- Communications
- Navigation
- Weather
- Battle Damage Assessment
- Missile Launch Detection and Warning

The first function, combat itself (the other six being combat-support roles), involves both attacks from space to earth (a future possibility) and antisatellite operations (a current capability). As weapons are placed in space or as terrestrial, sea, or aircraft-based antisatellite weapons are fielded, space will become another medium in which combat will occur or through which it will be propagated. When it does, space will be, in essence, a "mature" medium for warfare, just as land, sea, and, most recently, air have been. Like them, space will have its attendant strategies and doctrines, evolutionary and revolutionary.

The second space control function, space denial, is the converse of the first. Options for space denial may be considered to be bounded by the opportunities available to attack or otherwise negate either the space-based or terrestrial portion of an opposing space system. Using the terms "hard kill" (physical destruction) and "soft kill" (impairment of combat effectiveness by whatever means), we may list the following possible tactics.

- ***Satellite as target:***

Hard kill—Antisatellite (ASAT) systems including direct-ascent ASAT missile, anti-ballistic-missile missiles with ASAT capability, co-orbital ASAT, laser, directed-energy weapons, electro-magnetic impulse, etc.

Soft kill—Electronic warfare; deception and concealment.

- ***Satellite-related sites as targets:***

Hard kill—Attacks on ground sites.

Soft kill—Electronic warfare (including anticomputer options), political pressure, economic pressure, deception and concealment.

Antisatellite attack is what normally comes to mind when denying the use of space to an enemy is discussed. However, the options of space denial, broadly conceived, are more varied and allow a greater degree of flexibility than do ASAT operations alone. A course of action may be selected that is tuned both to the political environment of an emerging situation and the military outcomes desired.

If a satellite is the intended target, and a strong political statement through assured permanent destruction of that satellite is desired, then a hard-kill solution would be indicated. Currently, the only proven, operational ASAT capability resides in the Russian co-orbital system. The United States developed a homing ASAT missile, launchable from a specially configured F-15; after initial successful tests, however, it was discontinued as a result of congressional action. It is likely that the worldwide development of hard-kill ASAT weapons will continue,

although at a slow pace, and that various approaches will be explored, including laser, directed-energy sources, and kinetic-kill devices. For the near term, the Commonwealth of Independent States, especially Russia, and the United States will likely remain the only countries with the technical base and desire to develop such hard-kill weapons.

Other countries will presumably desire a hard-kill ASAT weapon, but they will find the soft-kill alternative more readily (if not currently) available, because of the simpler technological and industrial base it requires. If hard kill is either not feasible or not desirable (because of the political implications such an overt act may have), it is possible to negate satellites by electronic warfare (EW). In fact, unless satellites have been fitted with specific countermeasures, EW is perhaps the easiest means of putting them out of action. Electronic warfare provides four methods to counter a satellite: meaconing, interference, jamming, and intrusion (known collectively as MIJI).* While jamming is effective and is probably the simplest of these four methods to employ (and perhaps the easiest for the satellite's operators to detect and verify), the remaining MIJI options offer many possibilities for intentionally manipulating satellites or their data to the detriment of an enemy, and not necessarily with his knowledge. They present an opportunity to develop an entirely new area for deception operations.

The second major option for space denial is concerned with the terrestrial side of any space system. All space systems are supported by a variety of essential facilities, which include launch and control sites, communications facilities, and tracking assets. These facilities are possible targets for efforts to negate or degrade the usefulness of a space system, and they can be affected through either hard or soft-kill techniques.

If the actual destruction of the land portion of a space system is intended, politics are certainly a major consideration in the calculus of this decision. Depending upon the target and the method to be employed, the political cost of such an overt act may be prohibitive. In fact, it is possible that the portion of a satellite's terrestrial system to be targeted may be located not in the enemy's country but in the territory of a third party. Additionally, this facility may be owned by an international corporation or consortium that may have substantial international legal standing. This circumstance will become even more likely as more countries join consortia in order to pool resources for commercial space ventures (which may have inherent military applicability). An additional consideration in attacking a space-related terrestrial target is the means to be employed. Direct attack by easily identifiable military forces (such as aircraft or cruise missiles) may not be desirable; other direct options do exist, however, such as

* "Meaconing" is the deliberate confusion of navigation (especially air) by rebroadcasting radio beacon signals. See *Department of Defense Dictionary of Military and Associated Terms*, JCS Pub 1-02 (Washington: U.S. Govt. Print. Off., 1 December 1989).

insurgent, surrogate, or special operations forces. Each of these alternatives provides a degree of deniability that may be desirable.

There are other electronic, political, and economic approaches to space denial that are more attractive politically than the foregoing. They may even be useful for preventing conflict; by displaying resolve or by demonstrating the vulnerability of a potential opponent (especially one dependent on space systems), they may persuade an adversary to use means other than warfare. Soft-kill space denial avoids the need to rebuild a facility completely after the conflict is resolved, but it does not preclude resort to permanent destruction if the problem escalates.

The future will see a struggle for space control analogous to that in the twentieth century for air supremacy and the struggle for sea control that has been waged since the time of the ancient Greeks. In both cases, control of these mediums allowed the victor to "shape" the battlefield. Space has already served U.S. forces in conflicts of recent decades, but public acknowledgement of this fact has come only since Operations Desert Shield and Storm. What must also be recognized is that since American forces are heavily space-dependent, to retain the use of space must be a paramount consideration for U.S. planners in any future contingency. For the foreseeable future, conflicts will pit space-dependent U.S. forces against adversaries that have limited need for the medium. This asymmetry represents a potential Achilles' heel that could be exploited by a "space-smart" enemy; it would not be very difficult to do.

What is certain is that space, as a new medium or theater of military operations, is here to stay. If we are to prevail in this new environment, space control must become as commonplace to our professional mentality as the concepts of sea control and air supremacy. Failure to assimilate it may be disastrous, or at least seriously impede us, if we face an enemy who chooses to exploit our vulnerabilities. Space control will be as critical to future victories as air and sea control have been up to the present.

Ψ

[Robert E. Lee is] *too* cautious & weak under grave responsibility . . . wanting in moral firmness when pressed by heavy responsibility & is likely to be timid & irresolute in action.

General George B. McClellan
Peninsula campaign, April 1862