The US Army War College Quarterly: Parameters

Volume 19
Number 1 *Parameters 1989*

Article 10

7-4-1989

SIGNALS INTELLIGENCE AND NUCLEAR PREEMPTION

Robert D. Glassner

Signals Intelligence and Nuclear Preemption

ROBERT D. GLASSER

Some of the most violent superpower confrontations of the Cold War resulted from highly secret US military operations to collect signals intelligence (SIGINT) of the Soviet Union and her communist allies. In the two decades following World War II, US aircraft packed with sophisticated listening and photographic equipment routinely flew missions near and across the borders of the Soviet Union.[1] Indeed, on one occasion the US Strategic Air Command allegedly sent more than 50 planes over the Vladivostok area in broad daylight.[2] Between 1949 and 1965 there were more than 35 incidents in which US aircraft on these secret missions came under communist fire; 26 planes were shot down and more than a hundred American airmen were killed or taken prisoner.[3]

SIGINT collection has also occurred in more subtle ways. For example, after World War II the first gift given by the USSR to the American Ambassador to the Soviet Union, W. Averell Harriman, was a carved replica of the Great Seal of the United States in which the Soviets had secretly implanted a tiny listening device.[4]

The fact that serious risks have been taken to obtain SIGINT underscores the value the superpowers have attached to this important source of intelligence. Clearly, if a state is able to eavesdrop on the high-level deliberations of its adversary, much of the ambiguity concerning the enemy's intentions can be eliminated. In a superpower confrontation, this signals intelligence could be the single most convincing source of strategic warning of the enemy's intention to attack. As such, it might create a compelling rationale for nuclear preemption.

This article describes US and Soviet SIGINT collection capabilities. It outlines the main sources of breaches of communications security and how they might influence decisionmaking with regard to preemption in crises risking theater and strategic nuclear war.

Soviet and US SIGINT Collection

Most of the approximately 70 percent of US telecommunications that travel through the air by microwave or satellite[5] are vulnerable to eavesdropping. Moreover, this vulnerability is regularly exploited. According to the Deputy Director for Communications of the National Security Agency, "If it is going via satellite, you can presume the other guy is listening to it."[6]

The USSR makes a considerable investment in diverse platforms for obtaining SIGINT. Indeed, Moscow controls the largest SIGINT establishment in the world, employing over 350,000 personnel (as compared to the 60,000 to 70,000 employed by its American counterpart).[7] The two main Soviet agencies involved with SIGINT are the the KGB (Committee for State Security) and the GRU (Chief Intelligence Directorate of the Soviet General Staff). The KGB has responsibilities for intercepting both external and clandestine internal communications, deciphering foreign communications, and installing listening devices in foreign diplomatic compounds *within* the Soviet Union. The GRU's SIGINT operations, which are more extensive than those of the KGB, involve various fixed and mobile collection facilities inside the Soviet Union and abroad. The GRU additionally coordinates the SIGINT activities of thousands of Soviet military personnel.

Moscow relies on remarkably diverse platforms for SIGINT collection—e.g. satellites, aircraft, naval surface vessels, submarines, trucks, vans, automobiles, and fixed ground stations.[8] A worldwide Soviet SIGINT satellite system has existed since 1967.[9] The current system involves six satellites separated from each other by 60 degrees. They are believed to focus on intelligence relating to Western radar systems rather than communications per se. Soviet aircraft involved in SIGINT include over 20 varieties of military planes, like the Tu-95 Bear and the Tu-26 Backfire, and civilian aircraft managed by the national airline Aeroflot. The latter allegedly monitor VHF and HF bands along certain European flight paths.[10] The USSR's fleet of SIGINT

Mr. Robert D. Glasser is currently a Fellow at the Center for International and Strategic Affairs of the University of California, Los Angeles. He attended the Strategic and Defence Studies Centre of the Australian National University, from which he will receive the Ph.D. degree later this year. His dissertation was titled "Preemption in the Nuclear Age." This article was written while Mr. Glasser was a Visiting Scholar at the Cornell University Peace Studies Program. The author is indebted to Desmond Ball for comments on an earlier draft.

---

naval vessels, which is larger than that of the rest of the world combined,[11] monitors civilian and military communications and other signals relating to Western naval exercises, missile tests,[12] deployments, and operations.

Moscow's ground-based SIGINT operations have involved both fixed and mobile platforms. The mobile platforms have been most active in Europe and North America. West Germany has been a particularly important target for their activities. Thousands of Soviet-bloc trucks, vans, and mobile homes cross into the West each year to engage in SIGINT collection. In addition to monitoring important Western civilian and military communications, the vehicles conduct photographic reconnaissance of NATO military facilities, often from the very outskirts of the facilities themselves. Supplementing these mobile land-based vehicles are more than 500 fixed SIGINT facilities located within the USSR and abroad. The largest of these on foreign soil is located near Havana, Cuba. Its 28 square miles of antenna fields and satellite receivers (manned by some 2000 Soviet personnel) enable Moscow to intercept much of the US military and civilian communications traffic into and out of the United States.[13] Other fixed centers of ground-based SIGINT collection are Soviet diplomatic compounds around the world. According to a recent defector, one of these facilities, in Glen Cove, New York, ships tons of transcripts of intercepted telephone and telex calls to Moscow each year.[14]

The US SIGINT effort[15] is not as large as that of the Soviet Union, but it benefits from superior technology for processing, distributing, and transmitting the intelligence that is collected.[16] A number of US agencies are involved in SIGINT, including the National Security Agency, the Central Intelligence Agency, the National Reconnaissance Office, and the intelligence branches of the military services. The NSA's two main missions are securing US communications and collecting and processing foreign SIGINT. The agency maintains over 200 listening posts worldwide, in China, Alaska, Turkey, Norway, West Germany, and elsewhere.[17] The CIA and the military intelligence branches cooperate with the NSA in manning many of these listening posts. The CIA also conducts wiretapping and participates in satellite SIGINT programs. The National Reconnaissance Office functions on behalf of the other intelligence agencies; it is charged with operating and maintaining all American space-based SIGINT assets. It regularly produces a reconnaissance manifest which outlines the terrestrial targets for SIGINT collection.

America launched its first SIGINT satellite in 1962.[18] Since 1970, it has successfully launched some 12 geostationary SIGINT satellites. As with the Soviet systems, the American satellites can monitor radar emissions and intercept telephonic, radio microwave, and UHF communications. They can record and retransmit communications and other intelligence on demand. Today at least four of these satellites are deployed.

Additionally, aircraft such as the RC-135 and naval vessels are used for SIGINT collection. Since 1959, for example, US submarines have deployed

inside Soviet territorial waters to "tap" undersea cables, monitor missile tests, and conduct other operations.[19] American surface ships such as the USS *Yorktown* also have participated in recent SIGINT activities.[20]

This diverse network in space, on land, on and under the oceans, and in the air provides a truly phenomenal quantity of intelligence data. It is estimated, for example, that each year the National Security Agency produces millions of miles of taped intercepts and classifies between 50 and 100 million documents. Its production of classified waste material alone amounts to almost 40 tons a day.[21]

Sources of Security Breaches

These SIGINT capabilities have on occasion enabled each superpower to compromise the other's communications at the very highest levels of government. Breaches of security have occurred, in spite of the existence of options to encrypt sensitive communications, for three main reasons. The first, stated quite simply, is carelessness: officials have unwittingly assumed that a particular means of communication was secure when it was not. For many years, for example, Ambassador Harriman, unaware of the Soviet bug above his desk, spoke freely in his "private" office.

Apparently US officials were also negligent during the Cuban missile crisis, as shortly after the confrontation Khrushchev complimented the GRU for having provided him with telephone intercepts from Washington that had revealed to Khrushchev the events and discussions in official US circles.[22] The USSR has at times been comparably careless. On one occasion, for example, Washington was able to monitor the final emotional conversation between Soviet cosmonaut Vladimir Komarov and Soviet Premier Aleksei Kosygin, seconds before the cosmonaut's spacecraft, which had malfunctioned and was clearly doomed, began its final descent.[23] On another occasion equipment in the US Embassy in Moscow in the early 1970s allowed American agents to intercept the radio conversations of Soviet officials as they drove around the city in their limousines. According to one source, "We learned a little about their attitudes in the SALT talks and got some idea about the relationships between leading personalities."[24] In another incident, a conversation between Soviet leader Leonid Brezhnev and a Russian nuclear weapons expert allegedly revealed "that the Soviets planned the development of a new giant SS-19 nuclear missile, then unknown to US negotiators, and placed a loophole in the [SALT I] agreements that allowed for its deployment."[25]

Malfunctioning encryption devices have been a second source of communications leaks. This was demonstrated most recently in 1983 when the Soviet Union shot down Korean Air Lines flight 007. The Deputy for Air Defense at a district headquarters in the far eastern Soviet Union attempted to contact the Soviet General Staff on a secure phone to receive instructions with

regard to the airborne intruder he had detected on radar. However, the secure telephone system was malfunctioning. After trying three times to make the connection and failing, the official finally resorted to an open line which, of course, was monitored by the NSA.[26] As a result, the NSA has detailed transcripts of many of the important conversations that occurred during the incident.

The United States has had its own problems with malfunctioning security devices. In 1985 the failure of the scrambling equipment on board Air Force One enabled amateur radio operators, and presumably the Soviet Union, to eavesdrop on a discussion between President Reagan and Defense Secretary Weinberger in which military plans were detailed to divert some hijackers to Sicily.[27]

A third source of leaks involves those communications initially transmitted in encrypted form but which are nonetheless compromised because the encryption procedures have themselves been compromised. Take the case of retired Navy Warrant Officer John A. Walker and his friend Navy Code Clerk Jerry A. Whitworth.[28] The two passed highly classified US cryptographic information to the USSR for more than ten years before they were discovered. The Soviets meanwhile had intercepted and taped thousands of sensitive but encrypted US naval communications. With the assistance of Walker and Whitworth, Moscow has been able to decode this important intelligence.

Theater and Strategic Nuclear Preemption: The SIGINT Role

In a crisis each of these three sources of communications leaks could provide a state with invaluable information concerning its enemy's intentions. Indeed, even if a state could not understand the information it was intercepting due to encryption, increases in traffic *volume* to and from critical locations could be meaningful in itself. As one author has noted, "A sharp increase in traffic to and from Tyuratam, for example, may indicate an imminent space launch; a sudden switch into a high-grade cipher system or unusual jump in priority by units stationed along the border with Afghanistan may mean the outbreak of hostilities."[29]

SIGINT might be a particularly valuable means by which the Soviets could anticipate NATO's first use of nuclear weapons in Europe. NATO communications have been compromised for various periods since at least the mid-1950s. Recently declassified documents indicate that clandestine listening devices were discovered in the Main Conference Room of the European Command Headquarters as early as 1956.[30] At the same time it was disclosed that at least 14 telephones at the headquarters were equipped with jumper circuits which kept the telephones "alive" when the receivers were in their cradles. About ten years later, it was revealed that the Deputy Chief of NATO's logistics division, a West German rear admiral, had been an agent for Moscow.[31] NATO's operations apparently remain vulnerable today. The former Assistant Chief of

Staff for Communications and Electronics of the Supreme Headquarters Allied Powers Europe has recently asserted that "all NATO communications are indeed on a daily basis easily intercepted."[32]

The three nuclear-capable US unified and specified commands involved with NATO missions are the Atlantic Command, the European Command, and the Strategic Air Command. In a confrontation, these commands would employ four main systems to request the authorization for the use of nuclear weapons: the Improved Emergency Message Automatic Transmission System, the Automatic Digital Network (AUTODIN), the Automatic Secure Voice Network (AUTOSECVON), and the European Command and Control System. In addition, four NATO communications systems[33] might be used: the Status, Control, Alerting, and Reporting System; the Selective Release Improvement Program; the NATO-wide Communication System; and the Pilot Secure Voice Program. All of these systems are "secure" systems. However, the procedures for the release of nuclear weapons to NATO can be so time-consuming, perhaps requiring many hours,[34] and would involve so many different individuals and preliminary communications that security cannot be guaranteed. Former SACEUR General Bernard Rogers once explained the procedures he would follow in obtaining the release of nuclear weapons for use in Europe:

> Now the system that is used . . . is that I go to the political authorities at NATO headquarters with the request. I go also to the Ministers of Defense of all nations and I go also to the two nuclear powers simultaneously with my request for release. But prior to that time there would have been a warning message that I was probably coming to ask for release. And even prior to that, in order to get the political authorities thinking in terms of giving this permission, I would have sent what I would call an "early notification" message to them. So there is a series of steps taken.[35]

It is no surprise, therefore, that the Soviets have often been able to anticipate simulated nuclear use during NATO exercises, as one congressional official relates:

> When I was at the 1976 Reforger exercise, we were talking at the time with people in the field. The people in the field advised me of 12-, 13-, or 14-hour turn-around times from when they put in a request to use tactical nuclear weapons until the complete cycle had been completed. In fact, to embarrass us, the Soviets, who listen in on all our communications over there, announced two hours before we had, that is, before our troops had gotten approval, that NATO was going nuclear during the exercise.[36]

It should be pointed out, however, that the decision-lag problems associated with weapons dispersal may decrease somewhat when the Treaty on Intermediate-range Nuclear Forces is implemented. With the withdrawal

of Pershing 2s and ground-launched cruise missiles, NATO will rely on aircraft-delivered nuclear strikes and short-range nuclear weapons such as nuclear artillery rounds. In the case of the strike aircraft, the nuclear warheads are collocated with the aircraft even in peacetime. Nevertheless, given Soviet SIGINT capabilities, drawn-out NATO deliberations for first use could provide the strategic warning necessary to enable the Soviets to preempt.

Communications involving the strategic forces are similarly vulnerable. Donald C. Latham, the former Assistant Secretary of Defense for C^3I, has complained that the Russians "are eating our lunch when it comes to communications security on the battlefield, strategically, and between [weapon manufacturing] companies."[37] At least through the 1970s, Pentagon officials described the Strategic Air Command's communications as neither reliable, secure, nor survivable.[38] And this is not a uniquely American deficiency. Communications between the Soviet Fleet Command and Soviet ballistic missile submarines (SSBNs) have been monitored by Washington in the past. This monitoring alerted Pentagon officials to the fact that an explosion had occurred aboard a Soviet *Yankee*-class SSBN in 1986.[39] Similarly, during the trial of NSA computer analyst Ronald Pelton, it was revealed that the NSA had placed a listening device inside the Soviet Embassy in Moscow and had tapped a critical Soviet undersea communications cable located between the Soviet east coast and the Kamchatka peninsula. The tap enabled the NSA to intercept command and control information flowing "from the highest level of the Soviet Union down to the next level."[40]

In the United States, strategic nuclear execution orders are sent in the form of Emergency Action Messages (EAMs). EAMs are also used to direct changes in the defense readiness condition of one or more of the unified and specified commands, to test communications, and as part of war simulations.[41] They use special formats and communications means to speed the flow of information.[42] The United States and the Soviet Union can each quite easily intercept each other's EAMs. Amateur short-wave radio operators in the United States, for example, routinely monitor the Strategic Air Command's EAM transmissions,[43] and an assessment by the US military of Soviet SIGINT capabilities during the October 1973 Middle East War concluded that the Soviets had little difficulty intercepting American EAMs.[44] Ordinarily, these high-level communications are transmitted in special codes to prevent their compromise even if intercepted (although during the 1973 Mideast conflict at least one EAM—transmitted on 26 October—had only the first letter encrypted with the remainder in plain text[45]). In the past, even with some encryption, it was reportedly possible for an enemy to distinguish between those messages sent solely to test communications and those that resulted in action by the recipients.[46] Apparently, this deficiency has today been considerably corrected.[47] Nevertheless, some information may still be gleaned from encrypted US strategic communications based upon such peripheral aspects

AP/Wide World Photo

In May 1960 US Ambassador Henry Cabot Lodge displayed for the UN Security Council the bugged wooden replica of the Seal of the United States that had been presented by the Soviets to the US Ambassador in Moscow years earlier. Here he points to where the aerial for the listening device was located, "Right under the eagle's beak." Lodge offered the plaque as a "concrete example of Soviet espionage."

as originator, destination, priority, classification, appearance, number groups, format, length, etc.[48] During one major US exercise in 1979, for example, it was reported that more than 75 percent of the high-priority messages were shorter than routine exercise messages.[49]

There is, moreover, the slim possibility that an adversary might get hold of intelligence information (through spies or from other sources) that would enable him to make more sense of encrypted messages than would otherwise be the case. In 1983, for instance, highly classified US government data involving nuclear missile launch commands and wartime bomber routes was inadvertently fed over unsecured commercial telephone lines from one computer facility to another.[50] It is unclear whether the Soviets were able to intercept the data or, if they did intercept it, how useful they found it. However, the event demonstrates that highly damaging leaks of this kind are possible.

It seems unlikely that either superpower would be able to preempt in response to EAM intercepts that indicated the adversary was about to launch

a strategic nuclear attack. The interception and decryption of the EAM probably would not occur fast enough. Successful preemption would require one side to intercept and decode the enemy EAM, issue its own orders, launch its weapons, and destroy or disarm the enemy before that enemy could receive the EAM and execute his own strike. Since the forces on both sides can probably receive and execute nuclear war orders in minutes rather than tens of minutes, preemption would be extremely problematic. In any case, the military incentives for strategic nuclear preemption, given the huge and relatively invulnerable nuclear arsenals deployed by each superpower, have diminished markedly (some would say vanished) in the past few decades. The consensus among experts is that even after a preemptive strike that succeeded in disrupting command and control and destroying some nuclear weapons on the ground, the aggrieved power would be able to mount a counterattack that, although uncoordinated, would be devastating.

Even so, the significance of this intelligence should not be underestimated. EAM intercepts would, for instance, supplement the existing tactical early warning network of space-based optical sensors and ground-based radars, thereby validating warnings from these sources and increasing decisionmakers' confidence in retaliatory options such as launch on warning and launch under attack.

Conclusions

The superpowers have each made multibillion-dollar investments in SIGINT capabilities. Their investments have resulted in impressive and diverse systems that have, on occasion, enabled each to intercept the other's communications at the highest levels of government. Moreover, the superpowers routinely intercept vast quantities of lower-level communications and electronic emissions that reveal intelligence concerning the adversary's radar signatures, logistics, order of battle, and additional information that is useful in military planning.

In a superpower confrontation risking nuclear war, SIGINT and other sources of intelligence would become especially important. Leaders would anxiously sift through the intelligence for evidence of their adversary's state of mind: his sincerity, duplicity, or confusion. If the crisis deteriorated, SIGINT would become perhaps the single most convincing source of strategic warning of the enemy's intention to attack. This might facilitate Soviet preemption, particularly in the European theater where NATO deliberations on first-use could take many hours. However, preemption at the strategic level of warfare, even with the warning provided by SIGINT, would be problematic, given the rapid pace with which strategic nuclear attacks could be ordered and executed. In any case, each side's capability to launch ICBMs on tactical warning of an enemy attack, and the presence of numerous invulnerably

deployed submarine-launched nuclear weapons, suggest that the current military incentives for strategic nuclear preemption are at best uncompelling.

NOTES

1. For a description of these missions see: US Air Force Security Service, *A Special Historical Study of USAFSS Response To World Crises 1949-1969*, 22 April 1970 (declassified); John M. Carroll, *Secrets of Electronic Espionage* (New York: E. P. Dutton, 1966), pp. 134-96; and Dick van der Aart, *Aerial Espionage* (New York: Prentice Hall Press, 1986).

2. Interview with General Curtis E. LeMay, 2 December 1987, Newport Beach, Calif.

3. Carroll, p. 134.

4. Described in Carroll, p. 199.

5. NBC Nightly News, 19 August 1986, "Soviet Eavesdropping Techniques," reported by Anne Garrels.

6. Daniel J. Knauf, "Communications Security and the Problem of Hamlet: To Be or Not To Be," *Signal*, 39 (April 1985), 50.

7. Desmond Ball, "Soviet Signals Intelligence," *International Countermeasures Handbook* (12th ed.; Palo Alto, Calif.: EW Communications, November 1986), p. 73. See also Desmond Ball, "Soviet Signals Intelligence: The Use of Diplomatic Establishments," *International Countermeasures Handbook* (13th ed.; Palo Alto, Calif.: EW Communications, November 1987), pp. 24-25.

8. An excellent description of these platforms can be found in Desmond Ball, "Soviet Signals Intelligence (SIGINT)," unpublished paper prepared for the US Air Force Intelligence Service, Air Force Intelligence Conference on Soviet Affairs: The Soviet Union—Toward the 21st Century: Political-Military Affairs in the Gorbachev Era, Arlington, Va., 19-22 October 1988. The following discussion relies on this source.

9. In 1987 at least seven dedicated SIGINT satellites were orbited by the USSR. See Nicholas A. Johnson, *The Soviet Year in Space, 1987* (Colorado Springs, Colo.: Teledyne Brown Engineering, 1988), p. 74.

10. Jeffrey T. Richelson, *Sword and Shield, Soviet Intelligence and Security Apparatus* (Cambridge, Mass.: Ballinger, 1986), p. 98.

11. Ball, "Soviet Signals Intelligence (SIGINT)" (paper prepared for the US Air Force Intelligence Service), p. 37.

12. Andrew Rosenthal, "Tale of a Soviet Cap and a Missing Flight Recorder," *The New York Times*, 12 January 1989, p. A-20.

13. "Encryption, Survivability Improve Defense Communication System," *Aviation Week and Space Technology*, 9 December 1985, p. 80.

14. US Congress, Senate, *Report of the Select Committee on Intelligence*, Report 98-665, 98th Cong., 2d sess., 1 January 1983 to 31 December 1984, p. 34. See also, David K. Shipler, "Senator Says Russians Should Pay to Clear New Embassy of Bugs," *The New York Times*, 6 April 1982, p. 6. For an in-depth analysis of spying from Soviet diplomatic compounds, see Ball, "Soviet Signals Intelligence: The Use of Diplomatic Establishments."

15. For a good review of the Air Force's contribution to this effort, see *A Special History of USAFSS Responses To World Crises, 1949-1969*.

16. Bobby R. Inman, "Managing Intelligence for Effective Use," *Incidental Papers, Seminar on Command Control Communications and Intelligence* (Cambridge, Mass.: Program on Information Resources Policy, Harvard University Center for Information Policy Research, Spring 1980), p. 155.

17. The most comprehensive list available of the US SIGINT ground stations can be found in Jeffrey T. Richelson and Desmond Ball, *The Ties That Bind* (Boston: Allen and Unwin, 1985), Appendix I, pp. 315-33.

18. Desmond Ball, *Pine Gap* (Sydney: Allen and Unwin, 1988), p. 12.

19. Jeffrey Richelson, *American Espionage and the Soviet Target*, (New York: Quill, William Morrow, 1987), pp. 159-65.

20. Ibid., p. 166.

21. James Bamford, *The Puzzle Palace* (New York: Penguin Books, 1983), pp. 92-93.

22. Harry Rosetzke, *The KGB: The Eyes of Russia* (New York: Doubleday, 1981), p. 197.

23. Nicholas Daniloff, "How We Spy On the Russians," *The Washington Post Magazine*, 9 December 1979, p. 31. According to Daniloff the communications went as follows:

> Kosygin: (solemnly) "You and your kind made the greatest achievements in Russian history. We are proud of you. You will always be remembered."
>
> Komarov: (after a long pause, then screaming) "You've got to do something! I don't want to die!"

24. Ibid., p. 35, and Bamford, pp. 323, 359.

25. Walter Andrews, "Kissinger Allegedly Withheld Soviet Plan to Violate SALT I," *The Washington Times*, 6 April 1984, p. 1.

26. Seymour M. Hersh, "The Target Is Destroyed," *The Atlantic Monthly*, September 1986, pp. 66-67.

27. "Eavesdropping on the President," *Defense Electronics*, 17 (November 1985), p. 17.

28. Howard Blum, *I Pledge Allegiance . . . The True Story of the Walkers: An American Spy Family* (New York: Simon and Schuster, 1987). See also John D. Morocco, "Navy Master Plan Emphasizes Airborne ASW System," *Aviation Week and Space Technology*, 13 July 1987, p. 11.

29. Bamford, p. 127. See also Ball, "Soviet Signals Intelligence." Ball quotes a Soviet defector, Viktor Suvorov (pseudonym): "If a station we call C-100 springs suddenly into action even a child would realize that the battle readiness of the American troops in Europe was raised to a higher level."

30. Memorandum For: Chief of Staff, US Army; Chief of Naval Operations; Chief of Staff, US Air Force, Commandant of the Marine Corps, Subject: Clandestine Listening Devices, SM-176-56, 6 April 1956.

31. Rosetzke, p. 157.

32. Joachim M. Sochaczewski, "The Role of Communications in NATO," *Military Technology*, 8 (June 1984), 154.

33. The majority of NATO communications systems are 66-wpm teletype writers or printers with torn-tape relays.

34. See William R. Van Cleave and S. T. Cohen, *Tactical Nuclear Weapons: An Examination of the Issues* (New York: Crane, Russak, 1978), pp. 58-60. This source suggests 24 hours would not be unusual. However, the figure is derived from an Army field manual based on exercises in which the military was not moving with utmost speed.

35. Testimony of General Bernard Rogers Before the US Senate, Committee on Armed Services, *Department of Defense Authorization For Appropriation for FY83*, 97th Cong., 2d Sess., Part 7, Strategic and Theater Nuclear Forces, February-March 1982, p. 4334.

36. Anthony R. Battista, professional staff member, Research and Development Subcommittee of the Committee on Armed Services, US Congress, House of Representatives, Committee on Armed Services, Hearings on Military Posture and H.R. 6495, *Department of Defense Authorization For Appropriations For Fiscal Year 1981*, 96th Cong., 2d Sess., Research and Development, Title II (Washington: GPO, 1980), p. 1946.

37. Quoted in Edgar Ulsamer, "Top Priority For C^3I," *Air Force Magazine* (September 1986), p. 145.

38. See testimony of Dr. Gerald P. Dinneen, Assistant Secretary of Defense, C^3I, in Hearings Before the Subcommittee of the Committee on Appropriations, House of Representatives, 95th Cong., 1st sess., *Department of Defense Appropriations for 1978*, Part 3, Army Tank Programs, Research, Development, Test and Evaluation Communications Programs, Army Overobligation of Funds Reprogrammings, p. 745.

39. "3 Soviet Submarines Said to Patrol Atlantic 'Box,'" *The New York Times*, 6 October 1986, p. 6. See also Barry R. Posen, "Inadvertent Nuclear War? Escalation and NATO's Northern Flank," *International Security*, 7 (Fall 1982), 38.

40. See Mathew Wald, "NSA Man Alerted USSR to U.S. 'Ears,' Court Hears," *Sydney Morning Herald*, 29 May 1986, p. 9; Ronald Kessler, *Spy vs. Spy, Stalking Spies in America* (New York: Charles Scribner's Sons, 1988), pp. 178-219; and Robert Margolis, "The Exciting World of Radioteletype Monitoring," *Popular Communications*, October 1986, p. 48. For other examples of US SIGINT see Bamford, pp. 140, 201, 215-16, 254, 323, 359, and 381; and Ball, *Pine Gap*, pp. 53-54.

41. The Joint Chiefs of Staff send 40 exercise command messages each month. They conduct "system-wide" tests of the strategic communications system every three months and worldwide tests yearly. See Statement of Vice Admiral Huntington Hardisty, Director of Operations, Organization of the Joint Chiefs of Staff, US Congress, House of Representatives, Committee on Government Operations, *Our Nation's Nuclear Warning System: Will it Work if We Need It?* 99th Cong., 1st sess., 26 September 1985 (Washington: GPO, 1986), pp. 77, 130.

42. For more on EAMs, see Organization of the Joint Chiefs of Staff, *Detailed Analysis Report Exercise Power Play 79*, unpublished report prepared by the OJCS, 16 August 1979, Tab G; and William M. Arkin, "Nuclear War in Triplicate," *Bulletin of the Atomic Scientists*, December 1986, pp. 6-7.

43. Mike Chabak, "Your Guide to Shortwave Utility Stations," *Popular Communications*, March 1986, pp. 64-69; and Paul Vogt, "Fine Tuning the US Air Force," *Popular Communications*, August 1986, pp. 12-16.

44. *COMSEC Assessment During October 1973 Mid-East Conflict*, unpublished report prepared by Headquarters, United States European Command, ECJ6-A-73-0045-S, p. A-2.

45. Ibid., p. E-6.

46. Ibid., p. A-2.

47. Ibid. and author's interviews.

48. Bamford, p. 495.

49. *Detailed Analysis Report Exercise Power Play 79*, p. VIII-12.

50. Molly Moore, "High-Tech Security Failures Rise," *The Washington Post*, 8 June 1987, p. 1.