Next 5 Page(s) In Document Denied

attach to

80-2385

L-116

Declassified in Part - Sanitized Copy Approved for Release 2012/06/28 : CIA-RDP10M02313R000704030004-3

Next 1 Page(s) In Document Denied

14 OCT 1980

The Message Gap in Our Crisis Network

In a nuclear attack, would our leaders be certain to get through to the launch pads?

By Joseph Albright

SUNNYVALE, Calif. — Anyone driving by would have to wonder about the unprotected cluster of snow-white dishes pointing skyward along the Bayshore Freeway.

There behind a chain-link fence is one of the two or three U.S. military bases a president would need during any international crisis or hint of a Russian surprise attack.

It is the lone ground station from which the Defense Department controls the military communications satellites linking the president and America's distant forces and diplomats. It also steers most of the country's electronic intelligence, photographic reconnaissance and missile warning satellites.

No leak, no secret document, no disgruntled crypto clerk was needed to find the spot. All it took was page 20 of the unclassified posture statement which the Air Force sent to Congress last February. The Satellite Test Center at Sunnyvale is a "single point of control" for defense satellites, the statement reported. As a consequence, it said, the Defense Department's "current space operations are vulnerable to disruption."

A high-ranking scientific adviser to Defense Secretary Brown called it "unforgiveable" that such a critical base is "within bazooka range of a highway."

Sunnyvale also happens to lie in an earthquake hazard zone, with the San Andreas fault eight miles away. But to this adviser, at least, earthquakes are less worrisome than bazookas and satchel charges.

Sunnyvale is just one sample of a national security weakness that has been troubling professional military people, arms control advocates and some people in the White House — with good reason.

The problem is that in a nuclear crisis, the president cannot be sure of his ability to communicate with the commanders of his missiles, submarines and bombers.

No one is claiming that the Soviet Union can strike this country's command-and-control system with impunity, knowing for sure that the presidential "button" can be disconnected. S.J. Buchsbaum, a member of the Defense Science Board and chief of military communications for the Bell Laboratories, offered this much reassurance: "While there are various severe vulnerabilities that can and should be fixed, even today the system is sufficiently robust that it cannot be knocked out

However, Sen. Sam Nunn (D-Ga.) said: "The deficiencies in our present [communications] system pose a temptation to Soviet planners in a confrontation situation to be the first one to strike." And retired Army Gen. Alexander M. Haig Jr., former NATO commander, said: "I would place this area among the top priorities for prompt attention by the next administration."

In more dovish precincts, Paul Warnke, who was President Carter's first nuclear treaty negotiator, said: "If you really had the kind of command and control that is technically feasible, you would have even less reason to build the new MX missile."

Twenty years ago, the country got the jitters about a missile gap that turned out to be a myth. The present situation sounds even more preposterous. How could a nation that will spend $157 billion on defense next year — a nation that invented the telephone — fall prey to a message gap?

Vice Adm. Robert Y. Kaufman, director of command and control for the Navy, told a House subcommittee in May:

"It is a beautiful system in peacetime. We have literally 100 percent capability of getting the message to our submarines in peacetime. But when we get into varying types of wars, ranging from conventional through the gamut of nuclear wars, we get varying degrees of degradations."

He testified that the Navy's transmitting stations, including one in Annapolis, are "as vulnerable as a hand grenade on one of the antennas." Therefore, he said, the Navy also fields a "jury-rigged system" of overweight, aging radio relay planes.

The government does not call it a message gap. Its euphemism is "connectivity shortfalls," a phrase which surfaced in declassified testimony by Gen. Richard Ellis, commander of the Air Force Strategic Air Command.

Ellis told the Senate Armed Services Committee eight months ago that SAC and the Joint Chiefs of Staff, the Defense Science Board and the staff of the Chief of Naval Operations had uncovered such "connectivity shortfalls" in recent classified studies.

□ □

Where are these "connectivity shortfalls?" Here are some I have compiled in unclassified documents and interviews with generals, scientists and other communications specialists. The Pentagon has not taken issue with any of these findings.

• A president has 43 radio and telephone paths for dispatching one-way nuclear strike messages to one or another of the U.S. strategic nuclear forces. But questions exist about how many minutes any of these segments would endure after a Russian strike. "One of the weaknesses in the system is that the president doesn't have very long to make up his mind," said Lt. Gen. Kelly Burke, chief of Air Force research and development.

Even so, this year only one penny out of every $1,000 of the defense budget will go for procurement of equipment to strengthen the so-called Minimum Essential Emergency Communications Network, which is the most important cluster of channels among the president's 43 one-way paths.

• A president has much less standby equipment for the two-way conversations and conference calls he would need to determine whether the country really was under attack and what to do about it.

• The Joint Chiefs of Staff anticipate a "widespread l of connectivity" between the president and his comma ers in the opening minutes of a nuclear war. The ch said this loss would be caused by the powerful electrom netic pulses from a high-altitude nuclear burst wh would burn or upset electronic and computer circuits.

• The president has one $211-million "doomsday" co mand plane whose communications equipment is p tected against such pulses. But because of its maintena cycle, it can remain on alert at Andrews Air Force B only about 15 days a month.

At the president's disposal the rest of the time is an e lier "doomsday" plane that has about 2,000 openings the hull that could admit the damaging pulses. Boei Corp., which made the plane, has estimated that up 11,500 of the "mission essential" circuits in the old model would either sizzle up or suffer temporary failu after a high altitude nuclear burst even half a contine away.

Moreover, the Russians are aware of this vulnerabili and can determine when the "hardened" plane is on aler

• Of all "connectivity shortfalls," the most pressing how to strengthen the radio links with Poseidon and oth missile-firing submarines. A Navy officer said: "I suppo you could find a combination of [American] targets th would knock out our ability to communicate with the su marines . . . I don't think the interruption would be pe manent."

The fragility of submarine communications has this sic effect: At least some and probably all of today's U.S. mi sile submarines lack the kind of electronic "positive e able" fail-safe that keeps the Minuteman land-based mi siles in the president's personal grasp. The Navy has t rely on the discipline of its officers and a complicate launch sequence that reportedly requires concerted actio at half a dozen battle stations.

□ □

West Point cadets learn that communications has bee critical in warfare at least since the Battle of Cannae i 216 B.C., when Hannibal destroyed a Roman army by well-timed signal to his Libyan cavalry to attack th flanks of an advancing Roman wedge.

From World War II came more demonstrations of th leverage of information over brute force: lessons like th Battle of Britain, Pearl Harbor, Midway, the Battle of th Bulge.

The invention of atomic bombs and long-range missile imposed new non-negotiable demands on the nation' communications system. A recently declassified study b Richard Foster of Stanford Research International in cluded this ugly finding about America's vulnerability a of 1962:

"For example, it requires only 17 weapons to essentiall destroy the national command or, as an optional target, 1 weapons to destroy the national communications and pu the national command out of contact with the forces."

Foster, who is making similar studies for the Carter ad ministration, said it remains true that Washington and al

2

Our Crisis Network's 'Message Gap'

By Joseph Albright

This ground station just off a California freeway controls U.S. military communications satellites.

3

national command centers could be crippled by 19 warheads of 8 megatons each. Airborne command posts and other moving targets would presumably survive.

By contrast, his 1962 study said it would take 4,000 Russian intercontinental ballistic missiles to knock out most of America's nuclear retaliatory forces — and 200 American warheads would survive.

Some major improvements in communications have since occurred. These include military communications satellites, satellite-based missile warning sensors, long-wave radios being installed in command planes to pierce jamming and nuclear blackout.

□ □

At least part of the impetus for the Pentagon's recent "connectivity shortfall" studies was an early suspicion by President Carter and his staff that the system couldn't function in a nuclear war.

Last Nov. 15, Carter issued Presidential Directive 53 directing his subordinates to make sure the nation's telecommunications network could either survive or be reconstituted.

One requirement for the telecommunications system, PD-53 said, is that it "must provide for connectivity between the National Command Authority and strategic and other appropriate forces to support flexible execution of retaliatory strikes during and after an enemy nuclear attack."

Two contradictory themes run through the transcripts of this year's military budget hearings. One is that military witnesses are genuinely troubled about "connectivity." The other is that the PD-53 hasn't yet made much difference in Pentagon spending for communications equipment.

In an interview, Gen. C. Reuben Autery, director of command and control of the Air Force Strategic Air Command, said various radio, satellite, airborne command posts and other new systems will make a dramatic improvement in the emergency communications system by "1985 or thereabouts."

"Until those things are deployed, it is our opinion, and has been for some time, that the system is not as robust as it should be," Autery added.

How serious is all this? That depends on an appraisal of whether some Russian leader might launch a "bolt from the blue" first strike.

A most unlikely threat, say most U.S. military and civilian officials. Most tend to agree with Rand Corp. analyst Federick Sallagar that the major aim of the Soviet nuclear missile buildup has been "to undermine the strategic position of the United States by means short of war."

However, there is no question that Soviet strategists have thought about attacks on elements of America's command-and-control system, at least as recently as the late 1960s.

□ □

Some smart people have thought hard in the last few years about how to avoid a message gap. One thread that ran through two dozen interviews is that technology is available to fix the system.

Even with good management, the bill could run as much as a few billion dollars in each of the next five Pentagon budgets.

Some experts have suggested ways to give the taxpayer the most "connectivity" for the buck. These came in interviews at the Rand Corp., Stanford Research Institute, the Defense Nuclear Agency, the Brookings Institution, the Bell Labs and some other places that don't wish to be named. All these proposals are known to the Pentagon, and many are already receiving some low-level funding.

1. Guard the ground stations.

No one disagreed with the Pentagon scientific adviser who said it is "unforgivable" that the Sunnyvale satellite control site is "within bazooka range of a highway."

Step one: The Air Force should guard it like a Class A security installation, with rolled barbed wire on top of the fence, sensors to detect intruders and patrolling guards.

Better yet: Deploy a half-dozen mobile ground stations around the country, each capable of steering satellites.

Other "choke points" needing attention: the two satellite stations serving as the "downlink" for signals from U.S. missile warning satellites, one outside Denver and another in Woomera, Australia; a California site where an undersea cable from the Australia station comes on land, and the PAVE PAWS submarine missile early warning sites in California and Massachusetts.

When I first wrote about the situation of the satellite base at Sunnyvale, I omitted its location, thinking the Air Force had published a bit of harmful information by mistake. But the Air Force again identified the site as Sunnyvale. A spokesman said plans are proceeding to build a backup satellite control center in Colorado by 1985.

The Pentagon also said that the Air Force is reviewing its contingency plans "to mitigate impacts of disruption of [Sunnyvale's] operations" and is planning to begin upgrading the physical security of Sunnyvale "early in 1981."

According to "Jane's Military Communications 1979-80," the Sunnyvale site controls, among other space vehicles, the Defense Satellite Communications System, whose clients include the president, the Joint Chiefs of Staff, the National Security Agency, the Diplomatic Communications Agency and NATO.

2. The doomsday truck.

Improve the standby scheme for insuring that the president or someone in the line of succession survives a nuclear attack.

One way: Supplement today's doomsday plans by outfitting two dozen 18-wheel trucks as presidential command posts. Base them around the country and move them from time to time. Their wiring would be made of glass "fiber-optic" cables, which are not affected by electromagnetic pulses from distant nuclear bursts.

Inside would be radio transmitters with antennas tethered to pop-up balloons. In an emergency, helicopters would rush the successors to meet their designated doomsday trucks in rural areas unlikely to be targeted.

Also aboard each truck would be one of the Defense Advanced Research Projects Agency's experimental "antijam, antispoof, antiintercept" radios, called "packet radios." One would allow the president to broadcast virtually anywhere in the world.

4

...rival meter.

...the planners' migraines is how to tell who is ...mander-in-chief after a nuclear attack.

...possibility: A kit should be carried by the war... officer who shadows the president to hand him the ...clear launch codes. In the kit would be remotely-monitored instruments to record sudden increases in radiation or acceleration that would occur in a nuclear blast. If the monitors went off the scale, officials would prepare to swear in the vice president.

4. The piggyback network.

A nuclear attack targeted on the U.S. command and control system could chop up the Bell telephone network into isolated islands of communications, severing many of the Pentagon's critical leased circuits. There are backups, but each is somewhat vulnerable.

A further backup: Hang radio repeaters on thousands of commercial TV and radio station antennas throughout the country. Then add a computerized path-director to figure out automatically how to route a command signal across the country using undamaged repeaters.

5. The mobile ELF.

The two long-studied Navy projects for improving presidential communications with missile submarines would help somewhat.

One is a 158-mile network of Extremely Low Frequency (ELF) antennas buried in Wisconsin and Michigan. Another, which warrants higher priority, is Project Gryphon, a program to "harden" the Navy's radio relay planes against damage from electromagnetic pulses.

A more advanced idea: a mobile ELF transmitter network that couldn't be easily targeted. It apparently would consist of a network of trucks carrying radio transmitters. These transmitters would make up a grid several hundred miles long known as a phased array. The grid would be large enough to send the extremely long radio waves to reach deeply submerged submarines.

Military satellites, and much of the rest of the communications system, may be knocked out by electromagnetic pulses from a large high-altitude burst.

An answer: Put a standby communications satellite in one of the 16 missile tubes of each Poseidon submarine, giving each ~~sub one less~~ warhead.

7. Protect Ma Bell's backbone.

Although somewhat vulnerable in wartime, the Bell telephone system is considered the essential "backbone" system until the first missiles arrive. Now, some administration aides worry that the "backbone" may degenerate if pending bills aimed at "deregulating" the system pass Congress.

Over the years, Bell's long-lines division went along with Washington's urging that it bury key switching centers and install extra shielding so the system could function at least partially in wartime. Extra billions in design and construction costs have been passed onto consumers, never showing up in the defense budget. Bell went along because it was a monopoly.

A suggestion from some defense aides: If a deregulation bill passes, include provisions to insure that, in an emergency, the system can still function as one unit, responsive to the president. (Consumer advocates, including some in the White House, say the worries are exaggerated.)

8. Meteor burst messages.

What to do if all America's satellites are somehow disabled?

A possibility which has been known to be workable for 20 years: Bounce messages off the tails of meteors. Even long messages can be transmitted this way, but the sender must first wait for a meteor to pass near the earth. It happens quite often.

9. The anti-surprise attack treaty

The country's worries about a message gap derive in large part from the two or three Russian missile-firing submarines which reguarly patrol near Bermuda. Their missiles could hit Washington seven to 11 minutes after a launch, making an evacuation of the president virtually impossible. The Russian subs have been patrolling in those waters since the 1960s to counter American Polaris submarines, which have been poised for 20 years within 15-minute striking range of Moscow.

One military official proposes: Negotiate a treaty under which both superpowers agreed to keep their submarines at least 2,000 miles from each others' coastlines.

Navy officials oppose such a treaty, fearing restrictions on U.S. submarines; other U.S. officials say the Russians would insist on a ban against deployment of modernized U.S. medium-range missiles in Europe.

□ □

There is, of course, a 10th possibility. It is not appetizing: Let the president delegate his commander-in-chief's powers over the release of nuclear weapons.

President Kennedy once said on this subject, "I have not delegated to any one else the responsibilities for decision which are imposed upon me by the Constitution." But in 1964, it became known that the commander in charge of U.S. air defense fighters had been granted a limited delegation of "nuclear release authority" allowing his planes to shoot nuclear-tipped air-to-air missiles.

Haig, now president of United Technologies in Hartford, was asked whether he would favor moving in the direction of more nuclear delegations to others in the chain of civilian successors sent out of town in a crisis.

Haig replied: "You have to do that as well, and we do. It is provided for. The essence is always uncertainty, and not only in the nature of our response, but in the way in which that response would develop."

National Security Council spokesman Alfred Friendly Jr. has declined to say whether President Carter has delegated any of his nuclear release powers. A president technically could, according to an authoritative Library of Congress study, since they derive from his role as commander-in-chief.

Ergo, the sooner America solves its message gap, the easier it will be for a president to resist giving nuclear delegation orders to some Air Force general or Navy submarine commander.

5