the eastern iowa xerox exchange

eastern iowa xerox exchange -- eastern iowa xerox exchange
may, 1986 volume I number 1

in this our trouble we rise up, you and i,
acid falling from the sky,
as far away some people die for reasons
only known to selfishness.

all good passed down to us and you and me
could seep like water up a tree,
or so we dream that it could be that spring
will make some sense of winter.

tumble out your lonely words for us and them;
perhaps i can be a stem
for your leaf of personal zen and help
bring life to those around us.

The eastern iowa xerox exchange is a tentative newsletter, based principally on issues of war and peace and personal conscience. Its success of will be measured in recipient response, rather than monetary receipts. We are very nonprofit: donations are not required, but are welcome. We are uncopyrighted: no rights reserved. Written contributions and comments should be sent to our chief sifter, John Tinker, Box 66, Olin IA 52320. If you or someone else wishes to be added to our mailing list please white to our distributor, Franklin Seiberling, 199 6th Street #1, Coralville IA 52241.

FARMS NOT ARMS

*** DOOMSDAY GWEN TOWER *** 2 MILES EAST OF MECHANICSVILLE
MILEPOST 277 ON U.S. HIGHWAY 30

In the fall of 1985 the U.S. Air Force built a 300 foot radio tower on 15.5 acres of prime Iowa farm land. A component of the Ground Wave Emergency Network (GWEN), this tower is meant to be used after electromagnetic pulse and radioactivity black out conventional communications in the first minutes of a nuclear attack. In theory, GWEN would allow the government to continue fighting World War III even if most of us were already dead.

PEACE VIGIL *** NOON SATURDAY MAY 17, 1986

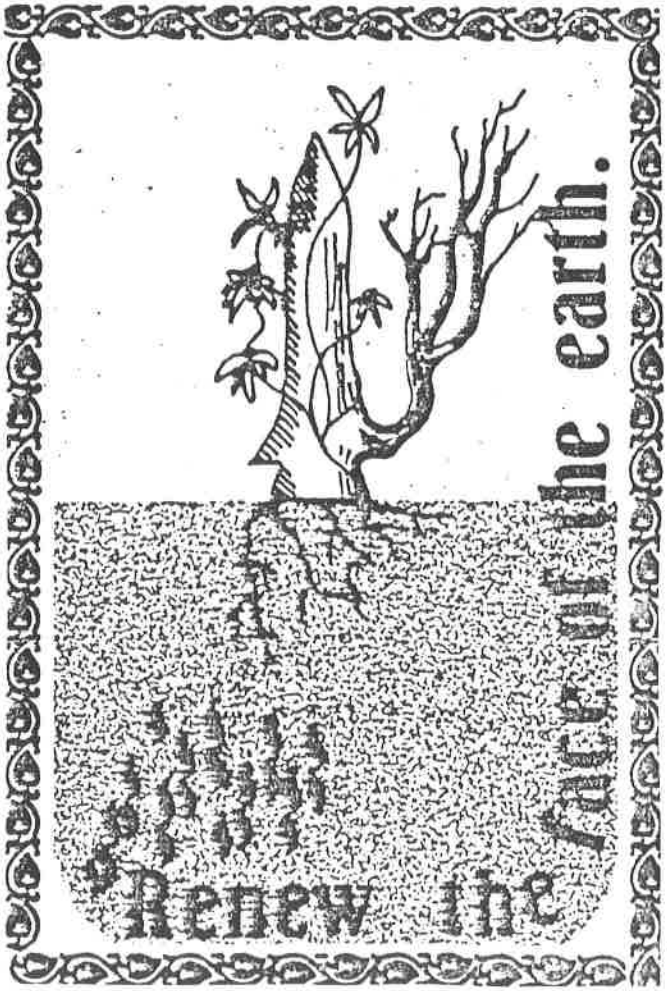
AN INVITATION

Come join us on Saturday, May 17 at noon at the GWEN site, two miles ease of Mechanicsville of Highway 30, in a silent vigil to witness to the life of spring and to the death symbol of the GWEN tower.

From 12:00 to 12:30 we will stand in a single silent line along Highway 30. At 12:30 there will be a discussion of our concern for the future of life and growth in Iowa where farms are going bankrupt and pessimism is deepening, while tax dollars are readily available for means of destruction.

For details, transportation possibilities etc. phone

Davenport: 324-0800 or
322-0150
Cedar Rapids: 854-7026



*** FOOD NOT BOMBS *** LIFE NOT DEATH *** PEACE NOT WAR ***

Value of Radio towers for Nuclear Orders Debated
N.Y. Times February 17,1986

Bruce G. Blair, an expert on strategic communication systems, questions the need for network of radio towers for nuclear war.

by Michael R. Gordon
Special to the New York Times

Washington, Feb. 16 -- A new network of radio towers designed to send warning information and retaliatory orders to United States nuclear forces is the focus of a dispute among experts over whether it could survive the opening minutes of a nuclear war.

Donald C. Latham, the senior Pentagon official in charge of command and communications programs, said in an interview that he believed the system could survive and should be expanded beyond current Air Force plans, to help the United States direct nuclear weapons in a war that could last days, weeks or longer.

He said that more of the towers should be built in the United States and that consideration was being given to extending the network into Alaska and Canada to communicate with bases for aircraft that intercept bombers.

But other Pentagon officials and some non-Governmental experts questioned the need for a large network, saying that both the radio system and the bases and command facilities linked to it would be among the first targets struck in a nuclear attack.

"Even if the system somehow remained intact, it would not have anyone to talk to," said Bruce G. Blair, an expert onstrategic communications systems, who recently worked for the Defense Communications Agency.

At the heart of the debate is the ground-wave emergency network of unstaffed radio towers that will transmit data using low frequency signals.

The Air Force plans to have 56 of the 300-foot relay towers operating by the end of this year, along with additional receiving and transmitting equipment at military sites, a spokesman said.

The entire network of 130 radio sites, already under construction, is to be completed by the early 1990's at a cost of $750 million. It would link bomber and aerial refueling tanker bases, missile launching centers, warning radars, facilities for airborne command posts and ground-based command centers.

Many of the towers are to be placed in regions that are remote from military centers, and the plans have aroused controversy in some communities under consideration for towers, such as Amherst, Mass.

Views of War Disputed

Antinuclear activists there have complained that the system would make their town a target and have charged that the system reflects the view that a "protracted" nuclear war is feasible.

Planning for the ground-wave emergency network began in the early 1980's when the Air Force sought a communications system to provide warning information to its bomber forces that would be resistant to

jamming and the disruptive effects of nuclear blasts.

But over the years the plans became more ambitious. The system is now intended to transmit retaliatory orders as well as warning messages.

Franklin C. Miller, director of strategic forces policy in the Defense Department's office of international security policy, said that the system would deter the Soviet Union from pursuing a strategy of interrupting United States communications early in an attack with high-altitude nuclear blasts to disable electronic components.

"The system is important for the first 35 minutes of an attack," he said.

But while many Pentagon officials agree with this, the Pentagon has not spoken with a single voice.

Initial Air Frce plans had called for at least 240 of the relay towers, instead of the 130 now planned, for an additional cost of $160 million, according to an Air Force spokesman. And Pentagon officials had talked of an eventual network of 400 to 500 radio sites.

Mr Latham, the senior Defense Department official in charge of command and control programs, said in an interview that the current plan "is an Air Force temporary position that I absolutely do not agree with."

"They came in and briefed me and I sent them back to the drawing boards to do a lot more analysis to show that they have not covered all the possible needs," said Mr. Latham, who added that the plan for 130 towers reflected budgetary concerns.

Doubts on Aid in a Long War

Mr Latham contended that the system needed to be expanded to make it more resistant to attack, adding that the Pentagon was reviewing a proposal to extend it into Alaska and Canada to link up with air defense units there.

A Pentagon official who asked not to be identified said that Mr. Latham's vision of a large network that could extend into Canada had not yet been formally endorsed. The official, who supports other communications systems intended to "endure" a nuclear strike, questioned whether the ground wave system would contribute to the American ability to fight a long nuclear war.

"If the Soviets wanted to attack the system they could do that and still have enough warheads left," he said.

Some experts agree with this. Mr. Blair said that some Defense Department studies justified skepticism that the network "could function coherently in the wake of any attack involving significant numbers of weapons unless the attacker decided not to target" the relay towers.

He said that the relay towers could transmit signals about 200 miles and that "tens of weapons" directed at specific relay towers would be sufficient to "dismember the network into essentially useless segments."

Mr. Blair said that he saw a role for the system in providing warning information to bombers but argued that there was no persuasive rationale for trying to build a system for a long nuclear

war because the bomber bases, missile fields, underground command posts and radar installations linked by the system were important and vulnerable targets and would be destroyed. The missile£carrying submarines, considered the element of the American strategic forces most likely to survive attack, are not served by the network.

But Mr. Latham argued that defense planners "have gone to extraordinary means" to make the system more "survivable" so that it could function after an attack. Such a capacity, he said, would help deter an initial attack.

Such measures involve equipping the towers with auxiliary diesel generators that would operate the transmitters for up to a week after regular power was lost.

Further, a switching system is used so that if some towers are knocked out, the network seeks out an alternative route.

Mr. Latham also noted that placing the towers in remore areas away from military centers lessened the chances that they could be attacked. He argued that the Soviet Union would not try to attack a large system because it would be likely to want to use its most accurate warheads on other targets. "It is hardly worth trying to target those towers." he said.

Air Force officials who oversee strategic communications programs declined to be interviewed. Asked about Mr. Latham's criticism, the Air Force issued a statement saying that as a result of "continuous studies," the plan had periodically been adjusted.

PROBING STAR WARS' COMPUTER QUAGMIRE

[Taken from the fall 1985 issue of NUCLEUS, published by the Union of Concerned Scientists.]

Of the several technological breakthroughs required to create a working Star Wars defense, one of the most remarkable must come in computer programming. Many computer professionals, in fact, believe that it will prove impossible to write software to track and identify many thousands of fast-moving objects in space, and then send defensive weapons to their marks -- flawlessly and within seconds. One doubter is David L. Parnas, a professor of computer science at the University of Victoria in British Columbia. Parnas, a US citizen, recently resigned from the Pentagon's advisory Panel on Computing in Support of Battle Management, whose job is to frame the computing tasks confronting the Star Wars project. With his resignation, Parnas submitted eight short papers outlining the computing obstacles that, be believes, make a Star Wars defense unworkable. [All eight papers appear in the September-October 1985 AMERICAN SCIENTIST.]

All software, Parnas notes, is to some extent unreliable, and bugs are routinely worked out during use -- yet the Star Wars system cannot be tested under realistic conditions and must perform without a hitch if called upon. The immensity of the program needed -- the Pentagon has estimated it at 100 million lines of code -- creates special problems. Despite attempts to develop new programming techniques more appropriate for mammoth projects, working programmers continue to use the conventional "think-like-a-computer" approach; unfortunately, this sequential method is unreliable for large, intricate programs. Finally, Parnas believes that the new technologies sometimes held up a cures for these software ills -- such as artificial intelligence, automatic programming (the use of computers to program other computers), and program verification (the use of mathematical proofs to establish that the program will work) -- do not in fact promise reliable software for Star Wars.

WHY THE SDI SOFTWARE SYSTEM WILL BE UNTRUSTWORTHY
by David Lorge Parnas

I. Introduction

In March 1983, the President called for an intensive and comprehensive effort to define a long-term research program with the ultimate goal of eliminating the threat posed by nuclear ballistic missiles. He asks us, as members of the scientific community, to provide the means of rendering these nuclear weapons impotent and obsolete. To accomplish this goal we would need a software system so well developed that we could have extremely high confidence that the system would work correctly when called upon. In the sequel I will present some of the characteristics of the required battle management software and then discuss their implications on the feasibility of achieving that confidence.

II. Characteristics of the proposed Battle Management Software System

1) The system will be required to identify, track, and direct weapons towards targets whose ballistic characteristics cannot be known with certainty before the moment of battle. It must distinguish these targets from decoys whose characteristics are also unknown.

2) The computing will be done by a network of computers connected to sensors, weapons, and each other, by channels whose behavior, at the time the system is invoked, cannot be predicted because of possible countermeasures by an attacker. The actual subset of system components that will be available at the time that the system is put into service, and throughout the period of service, cannot be predicted for the same reason.

3) It will be impossible to test the system under realistic conditions prior to its actual use.

4) The service period of the system will be so short that there will be little possibility of human intervention and no possibility of debugging and modification of the program during that period of service.

5) Like many other military programs, there are absolute real-time deadlines for the computation. The computation will consist primarily of periodic processes but the number of those processes that will be required, and the computational requirements of each process, cannot be predicted in advance because they depend on target characteristics. The resources available for computation cannot be predicted in advance. We cannot even predict the "worst case" with any confidence.

6) The weapon system will include a large variety of sensors and weapons, most of which will themselves require a large and complex software system. The suite of weapons and sensors is likely to grow during development and after deployment. The characteristics of weapons and sensors are not yet known and are likely to remain fluid for many years after deployment. The result is that the overall battle management software system will have to integrate a software system significantly larger than has ever been attempted before. The components of that system will be subject to independent modification.

III. Implications of these problem characteristics

Each of these characteristics has clear implications on the feasibility of building battle management software that will meet the President's requirements.

1) Fire control software cannot be written without making assumptions about the characteristics of enemy weapons and targets. This information is used in determining the recognition algorithms, the sampling periods, and the noise-filtering techniques. If the system is developed without knowledge of these characteristics, or with the knowledge that the enemy can change some of them on the day of battle, there are likely to be subtle but fatal errors in the software.

2) Although there has been some real progress in the area of "fail-soft" computer software, I have seen no success except in situations where (a) the likely failures can be predicted on the basis of past history, (b) the component failures are unlikely and

are statistically independent, (c) the system has excess capacity, (d) the real-time deadlines, if any, are soft, i.e. they can be missed without long term effects. None of these are true for the required battle management software.

3) No large scale software system has ever been installed without extensive testing under realistic conditions. For example, in operational software for military aircraft, even minor modifications require extensive ground testing followed by flight testing in which battle conditions can be closely approximated. Even with these tests, bugs can and do show up in battle conditions. The inability to test a strategic defense system under field conditions before we actually need it, will mean that no knowledgeable person would have much faith in the system.

4) It is not unusual for software modifications to be made in the field. Programmers are transported by helicopter to Navy ships; debugging notes can be found on the walls of trucks carrying computers that were used in Vietnam. It is only through such modifications that software becomes reliable. Such opportunities will not be available in the 30 minute war to be fought by a strategic defense battle management system.

5) Programs of this type must meet hard real-time deadlines reliably. In theory, this can be done either by scheduling at runtime or by pre-runtime scheduling. In practice, efficiency and predictability require some pre-runtime scheduling. Schedules for the worst case load are often built into the program. Unless one can work out worse case real-time schedules in advance, one can have no confidence that the system will meet its deadlines when its service is required.

6) All of our experience indicates that the difficulties in building software increase with the size of the system, with the number of independently modifiable subsystems, and the number of interfaces that must be defined. Problems worsen when the interfaces may change. The consequent modifications increase the complexity of the software and the difficulty of making a change correctly.

IV. Conclusion

All of the cost estimates indicate that this will be the most massive software project ever attempted. The system has numerous technical characteristics that will make it more difficult than previous systems, independent of size. Because of the extreme demands on the system and our inability to test it, we will never be able to believe, with any confidence, that we have succeeded. Nuclear weapons will remain a potent threat.

CHALLENGER'S HIDDEN FALLOUT

[By Anne Milner, from the May/June 1986 issue of SIERRA.]

If the space shuttle Challenger had exploded during its next launch, originally proposed for May, the results could have been even more catastrophic.

Karl Grossman, a journalism professor and author of the book COVER-UP: WHAT YOU ARE NOT SUPPOSED TO KNOW ABOUT NUCLEAR POWER (Permanent Press, 1980), says NASA and the Department of Energy (DOE) were planning to use the next Challenger mission to fire a space probe powered by 46.7 pounds of plutonium to explore the atmosphere of jupiter.

"A pound of plutonium has the theoretical potential to give every person on Earth a lethal dose of lung cancer," says Grossman. "The explosion of a shuttle with plutonium abord could affect millions of people through the wide dispersion of tiny plutonium particles."

After reading about the Jupiter mission ("Project Galileo") in a DOE newsletter last year, Grossman wrote to NASA and DOE for analyses of the consequences of shuttle accidents. "They gave me a very hard time, claiming the information was confidential," he says. Grossman subsequently filed a Freedom of Information Act request, and last April the two agencies were ordered to give him the documents he sought.

But it wasn't until last October, with help from Sen. Patrick Moynihan and the Fund for Open Information and Accountability, that he finally received hundreds of pages of information on the consequences of plutonium being vaporized in a shuttle explosion. The pages giving specifics on the number of people that would be affected were whited out, on the grounds that this data could pose a threat to national security.

"The release of this information is mandated by national INsecurity," Grossman says.

"Here we are, fueling space probes with one of the most toxic substances on Earth. We're just asking for a catastrophe to happen."

NASA has called the risk of releasing plutonium-238 into the environment small, "due to the high reliability inherent in the design of the Space Shuttle."

WHY WORRY ABOUT WATER?

[From the May/June 1986 SIERRA.]

Michael Castleman's review of Jonathan King's TROUBLED WATER: THE POISONING OF AMERICA'S DRINKING WATER (March/April 1986) assures us that a healthy fear of tap water is well advised. Common sense makes one wonder.

The government regulates trihalomethanes (THM), for instance, at a maximum level of 100 parts per billion in drinking water. Chloroform, the main constituent of THM, is said to be a carcinogen; it causes cancer in certain lab animals under certain test conditions. But a regular cup of breakfast coffee contains some 4,000 parts per billion hydrogen peroxide, plus some 4,000 ppb methylglyoxal, both known carcinogens. A 12-ounce can of cola contains about 7,900 ppb formaldehyde. Beer contains nitrosamines as well as formaldehyde. And so on. All are carcinogenic, all far in excess of anything in tap water, and all totally unregulated and unremarked by the Jonathan Kings and Michael Castlemans of the world. How come?

Robert M. Spangler
Littleton, Colo.