S. HRG. 105—445

RADIO FREQUENCY WEAPONS AND PROLIFERATION: POTENTIAL IMPACT ON THE ECONOMY

HEARING

before the

JOINT ECONOMIC COMMITTEE
CONGRESS OF THE UNITED STATES

ONE HUNDRED FIFTH CONGRESS

SECOND SESSION

February 25, 1998

Printed for the use of the Joint Economic Committee

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1998

cc 47-892

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-056562-6

CONTENTS

OPENING STATEMENTS OF MEMBERS

WITNESSES

SUBMISSIONS FOR THE RECORD

RADIO FREQUENCY WEAPONS AND PROLIFERATION: POTENTIAL IMPACT ON THE ECONOMY

Wednesday, February 25, 1998

UNITED STATES CONGRESS
JOINT ECONOMIC COMMITTEE
WASHINGTON, D. C.

The Committee met, pursuant to notice, at 10:00 a.m., in Room 106, Dirksen Senate Office Building, the Honorable Jim Saxton, Chairman of the Committee, presiding.

Present: Representatives Saxton and Ewing.

Staff Present: Vaughn Forrest, Darryl Evans, Colleen Healy, Mary Hewitt, Dan Lara, Juanita Morgan, and Andrew Quinlan.

OPENING STATEMENT OF REPRESENTATIVE JIM SAXTON, CHAIRMAN

Representative Saxton. If I could get your attention just for a moment, and if you would kindly take your places, we'll prepare to begin.

Thank you all very much for being here this morning. As you probably know, Congress, from time to time, looks at issues that have not received a lot of attention. Today's hearing is about one of those issues, and I think it's quite timely.

We have just concluded a chapter in our relationship with another country, namely Iraq, dealing with another set of weapons that I guess people are somewhat surprised exist in the magnitudes they do, basically chemical and biological.

It occurred to me when I was listening to the news on the radio this morning that given the arrangement that has apparently been agreed to between the United Nations and Iraq, that chemical and biological weapons will undoubtedly take a less prominent role in the news in the days ahead, simply because they have dropped out of sight to a degree.

On June 17th of last year, the Joint Economic Committee (JEC) held a hearing called Economic Espionage, Technology Transfers and

National Security. It spoke to another one of these issues that we believe are very important and don't receive enough attention.

In that hearing, we heard testimony from Lieutenant General Robert Schweitzer about a new class of weapons, radio frequency weapons (RF), and the impact of these new weapons on civilian and military electronic infrastructure in our country.

Since the General talked about a terrorist threat and a proliferation threat, the Joint Economic Committee has continued to investigate these potential threats, as they obviously have an impact on life here in general, and our economic life, in particular.

I am pleased to welcome to the Committee this extremely knowledgeable group of panelists, and I would like to introduce them at this time.

Dr. Alan Kehs is with the United States Army Laboratories, and will discuss the overall RF threat. Mr. Kehs has a B.S. and M.S. in Electrical Engineering, and an M.S. and Ph.D. in Physics from the University of Maryland.

He is a recognized expert on the generation and the use of intense relativistic electron beams for the production of high-power microwave radiation.

Recent assignments include the Chief of the Source Physics Branch of the Chief of Nuclear and High Power Microwave (HPM) Technology Office. Dr. Kehs has chaired the Eighth National Conference on HPM in April of 1997, and currently chairs the triservice HPM technology.

We will also hear from Dr. James O'Bryon. He is the Deputy Director of Operational Test and Evaluation Live Fire Testing with the Office of the Secretary of Defense at the Pentagon.

He has received a B.S. in Mathematics, and also has a graduate degree from George Washington University in Operations Research Management Science, and from MIT, through the Electrical Engineering Department.

The Director will discuss the role of live fire testing and how it will play a role in testing our military equipment with RF weapons.

Dr. David Schriner is the Principal Engineer of Directed Energy Studies with Electronic Warfare Associates, and a recently-retired engineer with the Naval Weapons Testing Facility at China Lake.

He has numerous patents, has received superior service awards, and has given technical presentations over 42 years of civil and military

service. He will discuss the difficulty in building an RF weapon, and the terrorist threat.

Finally, we'll hear from Dr. Ira Merritt, who is with the Missile Defense Space Technology Center in Huntsville, Alabama. He has more than 25 years of experience in developing advanced technologies, systems requirements, systems designs, and test capabilities for ballistic missile defense systems.

He has a Bachelor of Science in Chemical Engineering and advanced degrees in nuclear engineering. Dr. Merritt will discuss the proliferation of RF weapons, primarily from the former Soviet Union.

We look forward to hearing from each of you gentlemen during the hearing this morning, and at this time, we'll begin with Dr. Kehs.

[The prepared statement of Representative Saxton appears in the Submissions for the Record.]

OPENING STATEMENT OF R. ALAN KEHS, ARMY RESEARCH LABORATORY

Mr. Kehs. Thank you, Mr. Chairman, and Members of the Committee.

I'd like to thank you for the opportunity to shed some light on these widely ignored topics that you've chosen for these hearings.

I spent most of the last 20 years working on various radio frequency weapons technologies. As you noted, I currently serve as Chair of the Triservice High Power Microwave Coordinating Panel.

In general, our Security Classification Guide prevents us from discussing anything but the most generic concepts, and this is going to severely limit the depth of discussion if we remain at this unclassified, public-release level.

It's not deemed to be in our best interest to provide details on our programs, or roadmaps to weapons development that might assist rogue states such as Iraq, which you just mentioned, terrorists, and others who would eventually wish to use these weapons against us.

However, one does not need to rely on classified reports in order to appreciate the potential impact of radio frequency weapons, or, as they are frequently called HPM weapons. Everyone in this room has undoubtedly experienced electromagnetic interference to some piece of household electronics.

Some common examples are the effect of lightening strikes or automotive ignition noises on radio transmission, placing two computers too close to one another on a bench or driving under power lines while trying to listen to the radio, and so forth.

A step up from these minor inconveniences is the warning that we hear each time that we land or take off in an airplane. We all wonder, can a GameBoy or a calculator really cause serious problems to airplane electronics?

The answer, of course, is that a GameBoy or a calculator or cellular telephone is not usually sufficient to disrupt airplane electronics, but it can happen. As a result, we adopt a policy of better-safe-than-sorry, and shut down electronics during the more critical takeoff and landing segments of commercial air flights.

We've now asked the question, how much power does it take to create problems? Realistically, these questions can't be answered at the unclassified, full-public-release level.

But, more subtle, the question becomes, at what point do civilian electronic devices become weapons? And let us now shift from the lower power levels, the milliwatts and microwatts of GameBoys and cellular telephones, to the very high powers, the gigawatts or megawatts of commercially available radar systems, t.v. transmitters, and particle accelerator tubes, and this is the technology platform from which HPM weapons programs would be based.

Conceptually, an HPM weapon looks like a radio transmitter. There is a power source, a tube to generate the RF energy, and an antenna to radiate the energy appropriately.

The key technologies and final products have been under development for the greater part of this century, and are readily available on a broad range of markets. In the Army, we make extensive use of surplus radar and radio equipment for our experiments.

Military electronics generally contain some electromagnetic shielding and protection devices, even if they're not specifically designed to withstand an HPM attack.

Commercial designers are generally only concerned with the FCC limits on electromagnetic interference, and no one really knows how susceptible large scale commercial electronic systems might be to a concerted electronic attack.

These commercial systems include our banking and telecommunications systems, as well as oil and gas distribution and transportation systems, among others. Although these systems are designed to withstand the loss of a critical node, a concerted attack would cause unknown effects.

High power microwave technologies currently appear on the critical technologies list, which means they are flagged before we export anything. However, the required approvals have not slowed the technology transfer of increasingly powerful and sophisticated HPM technologies to overseas buyers.

The intelligence community will have to address the threat issues, but I believe that they will find that existing technologies are more than sufficient to support several potential applications in threat scenarios.

The growing U.S. dependence on sophisticated electronics for warfighting and domestic infrastructure makes us potentially vulnerable to electronic attack. By its nature, the Defense Department is compelled to confront such threats, however, the full range of our technological society is also at risk and much less aware of these potential threats.

That concludes my statement, and I would be happy to answer any questions that you might have.

[The prepared statement of Mr. Kehs appears in the Submissions for the Record.]

Representative Saxton. Thank you very much, Dr. Kehs. We will get back to you with some questions.

Let me apologize. I didn't mention at the outset that that little red and green light will go off after about 12 minutes.

So if we all can confine our statements to that length of time, it will give us an opportunity to get into some questions in a little while.

Dr. O'Bryon, do you want to proceed?

OPENING STATEMENT OF JAMES F. O'BRYON, DEPUTY DIRECTOR OPERATIONAL TEST AND EVALUATION, LIVE FIRE TESTING, OFFICE OF THE SECRETARY OF DEFENSE, THE PENTAGON, WASHINGTON, DC

Mr. O'Bryon. Thank you, Mr. Chairman. It's an honor to appear before the Committee today to discuss the role and mission of live fire testing, and specifically as it relates to the ballistic threat and the threats

posed by radio frequency and electromagnetic pulse and other threats, as a matter of fact.

As your letter to me indicates, these issues are of great importance to our nation, as well as the world. I would like to ask that my prepared statement be entered into the record in its entirety, and I would like to just extract from that prepared statement.

Let me begin by acknowledging the fact that a number of years ago, Congress recognized that there was a significant and growing need to realistically test our weapons systems to assure that they would withstand the rigors of combat to inflict the maximum effect on the enemy when used.

There's an old saying that we have in the office, "Better to sweat in peace than bleed in war," and we believe that very sincerely.

The legislation which was authored back in Fiscal Year 1986 and strengthened since that time, most recently with the Federal Acquisition Streamlining Act, moving the Live Fire Test Office under the Director of Operational Testing, requires that we prepare an independent report based on the realistic testing of all of our major weapons systems and weapons platforms that provide protection to the user.

To date, we have done thousands of tests and have prepared over two dozen reports to this Congress, to the House and Senate, the SAC, the HAC, the HNSC and the SASC.

Live fire testing has revealed a number of design flaws which, had they not been found and corrected in testing, would probably have resulted in a loss of life and at least loss of significant amounts of equipment.

These are the kinds of tests that, the only other way you discover the wrongs in these systems would be to wait for combat to occur, and then it's just a little bit too late to do the fixing.

Since this is the Joint Economic Committee, I'm sure you're interested in costs, how much this testing has cost as a way of measuring our output. Of all the tests we've conducted, not one of them on any given system has exceeded one third of one percent of the total cost of the system. That's the most expensive series of tests we've done.

So I think that the money spent has been well worth it, and the survivability and lethality of our weapons has been seriously improved.

The System Threat Assessment Reports, or STARS, as they are known, are prepared by the service proponents and approved by the DIA.

These documents, by DoD regulation, are the primary source document used to establish what these emerging threats are.

I'd like to just describe briefly what the three threat categories are: First of all, the one that comes to mind to most people is what I call the classical conventional threat or the ballistic threat. We're doing an awful lot of testing on.

There's another threat which we're not going to talk about today, which is the unconventional threat. And the JCS Pub 1-02 describes a conventional threat as anything that's not nuclear, biological, or chemical.

So when you subtract out these last three and you also account for ballistic threats, what's left? Well, what is left is a very, very important emerging threat, which we are calling directed energy: high powered lasers, low energy lasers, high powered microwave RF systems, things that can travel at the speed of light and can be widely proliferated.

These traditional threats have mostly populated the STARS with little in the way of directed energy to date.

Recent Defense guidance has made clear that other nations may very well choose to fight the United States asymmetrically. It's the word that's being used, avoiding a frontal assault because, obviously, we are the only superpower in the world today, as most people would acknowledge.

Rather, they might well choose to select a specific area of our potential vulnerability, for example, communications, or information warfare or a selective threat to attack us more effectively and more efficiently.

Recognizing that our nation, both militarily and commercially, is heavily dependent upon electronically produced, processed and transmitted information, it makes good sense to assume that any rogue nation could easily try to exploit this potential warfare area, what I am calling a niche warfare area.

The military, drawing much of its technology from the commercial world, and it's growing more and more as COTS and NDI become the rule rather than the exception, our military systems, whether they be tanks, ships or planes, are heavily dependent upon computers and computer systems.

I was with IBM back in 1961 and 1962, and I think I am one of the first people in the world to have used an interactive computer terminal. I like computers a lot, and I understand something about them.

Now, of course, they've gone from the Defense Department into the commercial world and now back again. There are computers to navigate, computers to communicate, to acquire targets and to home in on them.

In fact, some of our new fighter aircraft literally cannot fly, due to their aerodynamic instability, without computer controls. They'd fall out of the skies without them.

Destroying, disrupting, corrupting, or interrupting computer components could be very serious. As our computers become more and more miniaturized, by the way, and faster, and more proliferated, it may become feasible to attack these platforms through their potentially soft electronic components.

Mark Twain, I think, put it best. He said, "If you put all of your eggs in one basket, you better watch that basket." And that's what we're here to say today.

Are the technologies such as the introduction of non-metallic composite skins for aircraft and armor, while they might minimize weight, inadvertently increase vulnerabilities by eliminating what we call the Faraday cage, that metal cage which has traditionally provided a degree of protection from electronic disruption, the kind of disruption you feel when you drive your car across the bridge and the signal is canceled out due to the girders of the bridge around you.

We recently initiated a series of joint live fire tests, which I would like to share very briefly today, with the three military Departments to assess the effects of potential radio frequency (RF) weapons against our platforms.

While there has been a lot of RF testing over the years, these joint live fire tests are particularly interesting for several reasons. I'll list four this morning for you.

First of all, we're looking at the survivability of our platforms. Most efforts to date have been looking at the lethality of us against them and directing energy against the enemy. These are looking at our survivability, our vulnerability to other people using these things against us.

Secondly, the source is a transient, electromagnetic, broad-band threat. Most of the testing to date is done on a very narrow band spike.

The broad band can get inside of a lot more systems, especially those systems where the enemy might not know where they're operating, just build a broad band and try to hit more things, rather than a narrow band.

Thirdly, the test was conducted outside. Most of the testing to date has been conducted inside. You know that when you sing in the shower, it sounds great – well, it might sound great. But it sounds differently when you're singing outside in the parking lot.

In the same way, these systems behave differently inside, artificially, as opposed to outside in the real world – where wars are fought, typically.

Fourth, the tests were done against a fully operational target, not simply a component or set of a components, a completely operational system. What we're finding in live fire testing is not just the hard kill, but the soft kill, where the electronics go down. They can cause a mission kill very, very quickly.

Why did we pick the Huey Cobra? Well, because it's available. It's a system that's actually going out of the inventory and it's a system that we feel that if we can demonstrate a certain vulnerability to a rather antiquated, unsophisticated threat, perhaps our more sophisticated, advanced platforms could also have similar or maybe even greater problems.

Just three weeks ago, I and some 200 other people attended a meeting in the Russell Building sponsored by the National Defense Industrial Association, at which time the issues of information security and warfare were discussed.

The fact that some of our military communications are conducted over commercial lines was noted, in fact, a high percentage of them. Hence, what might first appear to be a civilian problem could also be a military problem.

Finally, because of the rate of change of technology in communications, computers, and sensors, as well as in lasers and radio frequency technology, the complexities of the issues are moving very fast and increasing.

I'm not here to say that the sky is falling, or that our weapons don't work. What I'm trying to say, in conclusion, is that the world is changing, the potential threat is changing, and our approach to designing and testing in this emerging world must change to meet it.

We have to realistically live fire test to these emerging threats to our military platforms and weapons. Thank you very much for the opportunity to testify, and I'll be happy to respond to any questions you might have.

[The prepared statement of Mr. O'Bryon appears in the Submissions for the Record.]

Representative Saxton. Thank you, Mr. O'Bryon, for a very articulate statement.

We'll move now to Mr. Schriner.

OPENING STATEMENT OF DAVID SCHRINER, PRINCIPAL ENGINEER, DIRECTED ENERGY STUDIES, ELECTRONIC WARFARE ASSOCIATES

Mr. Schriner. Thank you, Mr. Chairman, and distinguished Members of the Committee. It's a pleasure and an honor for me to be here today to testify on the subject of the Design and Fabrication of a Damage-Inflicting RF Weapon that could be done and built by backyard methods, as I call them.

I have built such a device and I have tested it recently, and it has turned out to be very effective at disrupting various targets that we've aimed it at. Now, when we get into the specifics of what we did and how far and what the wave form was, that gets to be classified, even though this was infrastructure material.

But I have proved that such a system could be built and probably used by what you might call a cyber warrior or an RF terrorist against infrastructure items such as financial institutions, computers, medical equipment in a hospital, possibly automobile equipment like ABS systems and air bags, all the sorts of things that are normally found in the everyday world that we live in.

Let me begin by saying that although I have worked for 42 years as a civil servant involved in generally high-end advanced development activities. I've never been working for the high powered microwave community. I've never used their types of funds.

Further, I have seldom ever been part of the established club that does the types of things that I've worked on. Generally, the efforts that I have worked on have been of a quick-reaction nature in direct support of some military need.

And my approach, generally, has been to just go and do it, rather than worrying about how to do it, or who should do it or when to do it.

This approach has been very successful. I've fielded many systems that have been of great value to the military.

This came from my early beginnings in high school and grade school where I built many science projects. I won science fairs. I've always had to build my own tools, and I came out of the old school where you build your own HAM radio equipment or sound equipment.

I grew up building things from scratch. I guess you would have called me, in high school, kind of a science nerd. But you know you have those kids around today. They're the kids down the street that can come by and program your computer for you. They exist today just as they did in my day.

Well, in January of 1997, I retired from Civil Service, from the Naval Air Warfare Center at China Lake, and I really became interested in some of the work that we did for Dr. O'Bryon on his live fire test program where we used one of these transient wave devices that we've been talking about.

And after looking at that technology, I thought that this is exactly the type of thing that a terrorist or an amateur might be able to do with readily available components, stuff you can buy at the hardware store or at Radio Shack.

So, I built some of these transient electromagnetic devices. You see one of them right here. You notice that it uses spark plugs for spark gaps.

In the photos that you have there, you see one that I built in about two weeks. I spent less than $500 on that thing, and the first time we turned it on, it worked. We tested it last week, and in 12 out of 12 times, it took down the target that it was aimed at, at a significant tactical distance.

So, that convinced me that this is really something that the RF terrorist could do and use against our infrastructure systems.

Now, you might wonder, where does one go to get the information to build these sorts of things that General Schweitzer testified could be used by an RF terrorist and just kind of driven around the block until something bad happened to the object that they were aimed at?

You don't have to get into classified records at all for it. In fact, you can go back to the turn of the century to some reports written by Heinrich Hertz, the guy who really showed you that radio waves exist.

And he published a document in 1893 that has a diagram in it that, if you were to build this thing and irradiate a computer or something with it, it would probably take it down. So, historically, the technology is well known.

Secondly, you can go to some of the various magazines around and you'll see in my paper that I gave you, this is an underground electronics advertisement, and there you can get for $5, plans of how to build a high-energy electromagnetic radiation plasma generator or a guided power EMP generator, all the sorts of things that we're really talking about that a terrorist could do.

Now, I have looked at some of these and they are pretty bogus, but it begs the point that the environment is ripe for people to want to try some of that stuff.

I've also worked on more sophisticated systems like this one. This one uses pressurized hydrogen. The one that you have in the photos just uses plain old transformer oil, and it's very simple.

The one you have in the photo is something that you would have in the back of a van or something. This device here is something that you would attach to like a 12-foot t.v. dish. You could then aim that at aircraft that were landing and taking off at the airport.

If we're really worried about what a cellular radio or a computer might do on an airplane, you must really worry about what something like this could do to it.

As Dr. O'Bryon said, you better guard that basket.

Thank you.

[The prepared statement of Mr. Schriner appears in the Submissions for the Record.]

Representative Saxton. Thank you very much, Mr. Schriner. We'll look forward to the question and answer period so we can perhaps discuss the hardware that you brought with you there a little bit further. Thank you.

Mr. Merritt?

OPENING STATEMENT OF IRA W. MERRITT, CHIEF, CONCEPTS AND APPLICATIONS DIVISION, U.S. ARMY, ARMY SPACE AND MISSILE DEFENSE COMMAND

Mr. Merritt. Mr. Chairman, Members of the Joint Economic Committee, I'd like to thank you for the opportunity to be here this morning and to offer testimony regarding the proliferation of radio frequency weapon technology and its significance to the operability of our high-value assets.

My name is Dr. Ira Merritt. I'm employed by the U.S. Army as Chief of the Concepts and Applications Division in the Army Space and Missile Defense Command.

Some of the opinions and conclusions I expressed in my statement are based upon my own past experience and observations, and are not necessarily those of the Army.

I have been active in survivability-related activities and projects for more than 15 years, and during this time, managed the Army's Missile Defense Survivability Technology Program, and I have chaired a number of electromagnetic environmental effects requirements boards for project offices.

Some of my principal responsibilities at this time are to develop innovative and advanced technologies for their application to missile defense projects, and to evaluate technologies, including these radio frequency weapons technologies that we are talking about today, to establish their significance to operability of our systems.

Our interest in radio frequency weapons has increased in the last several years as a result of the technology developments that have already been discussed briefly today, and the increased proliferation and expected increase in the susceptibility of our microelectronics to potential radio frequency weapon waveforms.

As semiconductors become smaller and smaller, and require less power, they're becoming more susceptible to external sources of radio frequency energy. We pay great attention now to the mitigation of radio frequency environments that we anticipate.

However, the waveforms produced by these RF weapons are very different from our normal design requirements and design waveforms. The chart to my left summarizes that conceptually.

The green region of the chart shows our current radio frequency mitigation design regime. The far left, the portion coming down being from nuclear electromagnetic pulse, and the other portion being from narrow band, nearby friendly sources.

The orange region represents typical ultra-wide band and high power microwave outputs. As you can see, these are well outside our normal radio frequency mitigation design practice.

Worldwide interest in radio frequency weapons has increased dramatically in the last several years, largely, as a result of the collapse

of the Soviet Union. This has also contributed to our increased interest in this area.

The Soviet Union had a large and diverse radio frequency weapon program, and elements of it continue today within the FSU countries. The Soviet program is not well understood, but our personnel are at the forefront of efforts to understand its scope and accomplishments.

The other figures that I have here, that are also in my written text, are pictures of four Russian sources that produce radio frequency weapon-like outputs. They are available on the open market, and I will discuss them briefly.

The first photograph shows a Ioffe Physical Technical Institute pulser. It's from St. Petersburg, Russia.

One of its commercial applications is to generate wide-band pulses for mapping underground images. The pulser is compact, it operates on batteries, and the solid state switch technology that it uses has been used to upset computers and other electronics.

I have an example of that kind of switch. We're not talking about anything very large. I also have examples of specification sheets from Ioffe Physical Technical Institute of commercial products that could be used for electronic disrupters as well as for legitimate commercial applications.

Another photograph shows an early model of RADAN. The name doesn't stand for anything that we are aware of, but it's a compact battery-powered accelerator. This is the RADAN.

It's capable of generating either ultra-wide band or high power microwave pulses. There was a recent article in a Swedish newspaper that refers to this as an electronic bomb. It's not explosive. We believe that the RADAN system is the system that they're talking about.

The next photograph is of the NAGIRA radar. This photograph was taken near Nizhny Novgorod, Russia, shortly before the system was bought by and shipped to the United Kingdom.

It was originally developed to detect low-flying and low-cross section aircraft, but it produces pulses of about 300-500 megawatts that are five-nanoseconds, or five billionths of a second, long. The Russians were concerned enough about these pulses interfering with their aircraft that their sure-safe distance was several miles from Nagira.

So, I think the point was made earlier that even sensors and/or devices that we typically think of as sensors in commercial products, can be tailored – under certain circumstances – to function as weapons.

The last photograph is of explosively-driven radio frequency munitions that have been described in recent Russian military and popular magazines. The articles have recently heightened the awareness of radio frequency weapons, and particularly this class of compact explosive-driven device.

This device was spoken of recently in a Russian television announcement that stated that Sweden had purchased drawings of this device and that they had successfully tested them.

So, even though significant amounts of new information is becoming available, large uncertainties and risks still exist with respect to the status and capabilities of radio frequency weapons.

I believe that a more comprehensive risk mitigation effort is needed to accomplish the task of quantifying these risks. We should characterize the expected electromagnetic environments that these types of devices can produce by analyzing and understanding these rapidly evolving technologies.

As you have heard earlier, we should conduct tests to evaluate and quantify the effects of short-pulse RF waveforms, that are most likely to be seen from these sorts of devices, on representative electronic components, subsystems and systems, and we should use the results of existing tests and new tests to guide the development of broadly applicable electromagnetic mitigation techniques.

So, in conclusion, although we cannot precisely quantify the risks presented by radio frequency weapons today, we do know that that risk is increasing. I believe that we should respond to that risk by developing near-term, low-cost and broadly applicable mitigation techniques.

These techniques could greatly reduce our susceptibility to radio frequency weapon environments, and so reduce the risks to our technological superiority that's absolutely essential to our military and economic preeminence.

Again, I thank the Committee for the opportunity to appear today to comment on the proliferation of radio frequency weapons technologies and their significance to our critical infrastructures.

[The prepared statement of Mr. Merritt appears in the Submissions for the Record.]

Representative Saxton. Thank you very much, Mr. Merritt.

Let me begin with a question that I guess I want to say is fairly evident, but let me ask it anyway.

Obviously, from what you have all said and from what we have learned previously, most any system that has a computer capability or other electrical capabilities, apparently, in some instances, can be affected by radio frequency weapons or devices.

Such facilities as airport towers, aircraft, landing and takeoff, or, I suspect, aircraft in flight, generally, computers at a financial center, i.e., Wall Street, nuclear reactor control rooms, emergency services for police, fire, medical services, telephone switching centers, all kinds of communications, water treatment facilities, and just – I guess we could just go on and list almost everything – government services, the Pentagon, weapons systems.

Are all these things true, Mr. Schriner?

Mr. Schriner. Well, Dr. Merritt's chart, there, that showed earlier the wide spectrum of the transient wave devices, it's clear that if you had any radio operating over that whole frequency range, all the way from below the FM band, clear up into the low microwave regions, that radio would be jammed every time one of these pulses occurred.

And if you simply made something that pulsed 10 times a second, you would not be able to use any radio in that frequency band. If you parked a system like that up in the hills down around Los Angeles, you would probably cause the air control there to go VFR, and that would be a catastrophe.

So, there are many examples of—

Representative Saxton. By VFR, you mean they'd have to just use sight?

Mr. Schriner. Yes. They would not be able to do air control. You'd have lots of airplanes flying around looking for something to do, and that would be just a very simple example.

More complex examples involve actually parking beside some critical infrastructure target, oh, maybe like the air control relay station and jamming his ability to communicate radar pictures.

Being able to take down a computer at Wall Street is another example.

As General Schweitzer testified earlier, a terrorist would not have to throw the switch and get it to happen right now. He could just wait until it happened.

Secondly, these things don't go bang. They don't make a big flash or anything. They're very quiet. There's really no way of knowing that you're being touched by them until something bad happens, and then you wouldn't know who did it.

I believe there are many things in our infrastructure environment that are highly vulnerable to these.

Representative Saxton. So, we can conclude that throughout our modern, high-tech society, there are innumerable targets that radio frequency waves could affect in a very dramatic, disastrous way?

Is it fair that we can draw that conclusion?

Mr. Schriner. Yes. I have proved that by testing as we have done.

Representative Saxton. Now, let me move to another question. That involves the degree of high-tech knowledge that is necessary, and the degree of high-tech equipment components, materials, that are necessary to produce an RF weapon.

Mr. O'Bryon. If I could comment on that, as part of our joint live fire tests begun a year or so ago, I directed China Lake and Mr. Schriner to put together a device using no government built parts, in other words, things that anyone could find, to put them together. And he literally put them together in his garage out in California.

So, as far as technology is concerned, he took a piece of a motorcycle and a piece of a microwave oven, some spark plugs and a few other things, and that's basically what can be done.

Now, if someone had access to much more high-tech things and purer materials and more highly-machined parts, obviously you could do better. But he has successfully tested his device and got some significant effects with what I call just backyard materials.

Representative Saxton. Mr. Schriner, you have a device sitting next to you there on the table.

Mr. Schriner. Yes, sir.

Representative Saxton. Would it be possible for you to describe what it is that you have put together there, what you've used in this device?

Mr. Schriner. Yes.

All of these devices—

Let me first make it clear that there are two types of high-powered microwave systems.

We have what I call the conventional high-powered microwave systems that the military has been developing for years and these are the ones that everyone is much more familiar with than this new kid on the block, as I call it, the transient wave device.

The transient wave devices all employ some sort of fast-acting switch, like a sparkgap, or as Dr. Merritt showed, semiconductor devices.

And as Heinrich Hertz showed, sparkgaps generated RF fields. The art then is to build a very fast sparkgap. And that's been the focus of most of the current work in that area.

This is just an example of how to make a very fast sparkgap and then it uses actual automotive sparkplugs for the elements of it.

Instead of having to machine expensive Lexan parts and very complex high cost approaches, I just said, gee, how could I do this with off-the-shelf components and I use sparkplugs as a sparkgap.

This is a sparkgap here, and back here I use ignition coils as the power supplies. And an ignition coil cannot pulse more than about 200 times per second, so I simply have four ignition coils driving four sparkplugs to charge the thing.

So this is basically the kind of thing that you would put into a dish antenna.

Whereas the one you have the photographs of is something which has its own antenna that you could put into a van.

So all of these things are just really sparkgap devices. We've known about sparkgaps for radio communications clear back into the early days of radio.

And they found that the sparkgap transmitters generated such a broad spectrum that they couldn't put many channels on the air, so this condition caused them to use more clean waveforms.

So today, as then, sparkgaps will jam all of your radios and do other disruptive effects.

Representative Saxton. Thank you.

Mr. Ewing has a question which we're going to move to now. He has to leave. We'll get back to this in a little bit more detail.

OPENING STATEMENT OF REPRESENTATIVE THOMAS W. EWING

Representative Ewing. Thank you, Mr. Chairman, and thank you to the panel for being here and your testimony. Certainly, if you haven't been focusing on it, it can be quite disturbing as to the potential out there.

How difficult would it be for an organization or any group to plan to disrupt services across the country at one time?

Mr. Schriner. You mean in a synchronized manner?

Representative Ewing. Yes.

Mr. Schriner. They would have to have multiple devices and then they would simply have to agree that they're going to turn them all on at the same time, and focus them at a set of specific targets.

That wouldn't be a hard thing to do. These things work as soon as you turn them on.

That one that you had the photographs of, when we used that against a target, sometimes just one pulse, of its 200-per-second, that it can make, would turn the machine off.

So it happens rather quickly.

Representative Ewing. So it would have to be a rather extensive plan to disrupt a number of different things all at one time?

Mr. Schriner. That's true.

Representative Ewing. Mr. Merritt, you mentioned in your testimony some possible protections that we could have against – are those realistic and doable and affordable, and can they really protect us from people who want to sabotage our system?

Mr. Merritt. There have been some successful developments already, and of course at a low level there are a number of developments going on in different places in the country right now.

One specific example that may be interesting to you is a liquid which can be applied to circuit boards and then, when it's heated, the material becomes conductive.

So it's a way of cheaply and very flexibly, within our existing manufacturing processes, applying a Faraday cage – or an electromagnetic shield – as we've talked about.

So the research program that I was just described demonstrated attenuation factors of from 10,000 to 1,000,000, over a frequency range from a few megahertz to a few gigahertz.

So, yes, there are simple low cost approaches like that.

Others need to be developed.

But we have reason to believe that it's a credible thing to do.

Representative Ewing. Is there quite a bit of effort, I assume in the government side, the military side and the private sector, to develop ways to protect against this type of interference?

Mr. Merritt. There's a very large effort, of course, to minimize electromagnetic interference and to ensure compatibility with the sources that we know about and anticipate.

The purpose, I presume part of the purpose for the hearings today, is to address whether this scope should be broadened.

Because, as was mentioned, the STARs (system threat analysis reports) do not have enough detail in them, in their specifications in general, for projects to effectively address this new class of device.

Representative Ewing. Thank you, Mr. Chairman.

Representative Saxton. Thank you, Mr. Ewing.

Mr. Schriner, if I can just get back to you for a minute.

What you have described there seems to be relatively simple stuff in the vernacular.

As you were describing the device that you have with you there, it reminded me of the days when I used to listen to my grandparents' radio in the living room, you know, one of those big ones with the speaker in the middle of it and all that, and something would occur in the house, and all of a sudden, you'd hear static.

Is this a similar type of interruption?

Mr. Schriner. Yes, it is.

And another example of that is, before they had resistive wiring for ignition systems in vehicles, your AM radio would have a lot if ignition noise on it.

Actually, when a sparkplug in a vehicle fires, it generates a transient electromagnetic signal of very high amplitude. In fact, those are detectable 100 miles away.

I built a system during the Vietnam war days that could detect those kinds of ignition signals at great distances, so it's not uncommon to find transient electromagnetic waves from ignition systems, mixers, razors, anything with a little motor that sparks.

Any time you have a spark, you'll have these kinds of signals generated.

Now, when you focus them and groom them to be radiated, as we do with some of these systems, you now would call it a weapon.

But in other words, it would just be an interference source.

Representative Saxton. I see.

So we have been able to demonstrate here that this could be a widespread problem, an issue that could, as Mr. Ewing pointed out with his question, could interrupt transmissions and operations across the country, given the right kind of an organized attempt to do so.

And when we held our hearing last June, it sounded like we hadn't progressed very far against protecting ourselves from these kinds of potential instances.

Is that still correct, or are we beginning to make some progress?

Mr. Schriner. Well, when you talk to someone who has the responsibility of fixing the problem, the answer that you generally get is, yes, we know there's a problem out there but we don't have the funding to go off and fix everything.

So what I've always said is that we really ought to have some kind of a program where we can measure our vulnerability and then fix those things that are critically important and then forget about most of it.

And I believe that's what we have to do. I believe that there are shielding techniques that could be applied. I believe that there are methods by which you can design the circuitry right in the first place to make it immune.

But those are cost factors and they don't come into play until there's some force out there that suggests that they should. And it's not until you find the vulnerability and give somebody a bad report card on it that they'll pay attention to that.

And I think that's true in the military side as well as on the infrastructure side.

Representative Saxton. Would you like to address this question, Mr. O'Bryon?

Mr. O'Bryon. I agree with that.

I think the bad news is perhaps that the problem might be rather widespread.

The good news is that, as Dr. Merritt has indicated, there are ways to fix it, and a lot of these fixes might not be very expensive. That's the good news.

The problem though is if you don't know there's a problem, obviously you're not going to know enough to fix it and then know how to fix it.

I would like to mention one other thing. There's a prevailing feeling that the only way you get electromagnetic pulse, if you will, is with nuclear weapons.

We tend to think of only nuclear EMP.

There is another element. Some say we're in the post-nuclear era. I'm not sure I personally agree with that, but I think a lot of people do. But you can get a non-nuclear EMP, non-nuclear pulse even from a ballistic event.

In other words, if one hits a tank or a ship or something similar, a non-nuclear EMP is generated which can influence electronics as well.

Some of them have been observed and some of them are significant.

So I want to make sure that everyone realizes that these things also can be generated in different wave forms simply from a ballistic event as well.

Representative Saxton. Mr. Kehs?

Mr. Kehs. I would like to make the point that the whole idea of protection is actually complicated by there's a division between protecting devices against being burned out and there's protecting devices against being upset.

And many times, if you just upset the device, instead of burning it out, you can do that at a much lower level, and that's sufficient for a military operation.

When you look at our infrastructure, it's probably much easier to bring down the system and make everybody go and reset everything, which could take several hours to reset the internet or to reset large parts of the communications system.

You haven't necessarily burned anything out or hurt anything, and so to protect against that kind of upset is a very different kind of thing than to merely protect it against burnout or permanent damage.

And when you get into looking at each individual system, and how someone might want to attack us, each thing is going to have to be looked at separately.

There's quite a bit of technology that exists to prevent burnout, and as Dave said, looking at what you would have to do to the circuits to make them more immune to upset is a larger problem.

Representative Saxton. Mr. Merritt?

Mr. Merritt. I'm not sure that I have a lot to add to those comments except that one of the things that we are addressing in the conductive liquids, or inks, that I just described as an example, are low-cost broadly-applicable techniques that might be used in commercial systems, including those commercial systems that have a military application.

I think what you also heard is that the effects of these RF weapons are unpredictable. There certainly are effects but their unpredictability is one of the reasons I believe that we need to provide techniques that are cheap enough to go into commercial systems, that are broadly applicable, as I say, and that will find commercial application and will have a general effect of reducing the impact of terrorist attacks against our infrastructure.

Representative Saxton. What kinds of devices or systems are we talking about?

Going back to Mr. Schriner, when he talked about interference from sparkplugs in automobiles, we used to have little devices that we could put somewhere on the engine, I've forgotten exactly what they were, but they eliminated to a large extent – are those the kind of devices that you're talking about, or just give a general idea of the physical makeup of the devices?

Mr. Kehs. Well, one possibility, like I say, I think one of the clearest, easiest ones to understand is if we could put a conductive film like those liquids on circuit boards, we can reduce, redesign and problems with manufacturing of our own computers where one piece of a circuit or a computer affects another.

Right now, in this fixed test process, we wind up redesigning often.

This would allow us to go in and just simply put a shield in place. Well that shield is not only going to be effective against our own self-generated RF, it will also reduce our susceptibility to external sources.

Another possibility that we're looking at is limiters. Combinations of solid state and plasma limiters perhaps, and these could be, we're looking at very small, low-cost devices that could be put between the antenna and the sensitive elements of receiver, for example.

And the goal there should be to be able to proliferate those to virtually every sensitive receiver on the battlefield. These would have very broad, tremendous applicability.

There's a significance difference also between these RF weapons and the nuclear EMP. The nuclear of course covers hundreds of kilometers. These are going to be very, very limited in their range.

So if you get beyond a very close proximity to most of these devices, the kind of shielding I'm talking about would pay great dividends, I believe.

Representative Saxton. So shielding is not necessarily something that is so difficult to develop, it's just the – how can I say – the determination to get some shielding in place.

And we can do that given the determination to do so.

Mr. Merritt. That, and when people talk about shielding, they typically think of EMP on strategic systems. And that was a very expensive process.

I notice that George Baker is here, and George and I had a program a few years ago to address this combined nuclear and RF mitigation problem.

And it is possible, we think, to address it in a relatively general way and in a less rigorous way than is required on a strategic system.

Mr. Schriner. I could add to that by saying that we need the motivation to do that, and the motivation just doesn't exist right now on a lot of the infrastructure stuff, medical equipment and all, because the people that design it have to get a product out the door at a certain price and, boy, if they don't have to put something in, they won't.

Another problem is that when engineers now design something, because the chips maybe cost only a penny apiece, he might use five computer chips of some sort in there to accomplish an object task that he could maybe spend a little more time and do with one transistor. But he won't do that because that costs a little more to do that than to put four chips in.

Well, those four chips are four windows of vulnerability perhaps. So there is no motive or incentive out there now for them to do it right.

And I think that once we start giving out some bad report cards on the performance of some of this, the commercial side will wake up to the need to do that and start doing it.

Suppression devices can be built into like the mouse plug, but they won't put that in until they're shown a reason to do it because the thing, right, might cost you $20 now. But, when they provide them in the quantities that they build computers in, it might only cost a penny.

So there's a lot of economic dynamics at work causing the vulnerabilities to exist, and the same economic factors I think will drive towards fixing them when it's apparent that we have the problems.

Representative Saxton. Have there been any problems? Can you give any examples of where radio frequency interruptions have occurred in say the last decade or so?

Mr. Schriner. There have been a lot of accidental ones. Many times a computer will go down.

A good example of this transient wave thing is, you know, when you walk across the carpet and shuffle your feet on a dry day, and touch your computer keyboard, you have actually generated one of these electrostatic discharges, and that's very similar to this transient wave thing.

So that's an example of how it can occur just right at home.

And I believe that there have been many examples of where aircraft have flown through fields and engines have turned off.

These are generally not reported.

There have been tests that I've seen where new technology like this causes the boards on the airplane to go up, or things to happen that were wrong. And right away, that may go black, or right away, somebody says, gee, I better fix that.

There's just no structure to collecting that information together to propose that there is a large problem until you start getting to doing the things like Dr. O'Bryon does on his Live Fire Test program.

Representative Saxton. Can any of the rest, any of the others—

Mr. O'Bryon. Well, there is an incident in the open. Obviously, as was mentioned by Dr. Kehs, much of this cannot be discussed in open forum, but there is an open incident regarding GPS.

I believe it originated up in the Syracuse, New York area, where there was some antenna testing on a Comanche Helicopter and, after the testing was done, there was a small source that was left on, at five watts, I believe, out of Rome Air Force Base, which ended up totally disrupting

the global positioning system (GPS) being used to land, commercial aircraft in Albany, NY, for a period of a couple of weeks.

And, as was mentioned earlier here, it's not only generating doing the signal, but knowing that it's being done and from where, that's difficult. It was finally tracked to a low-power transmitter that was accidentally left on.

Representative Saxton. It was left on over a period of time?

Mr. O'Bryon. Over a period of a couple of weeks.

Representative Saxton. And over that period of time, it disrupted the GPS signals?

Mr. O'Bryon. Right. There were, I guess, a dozen or more aircraft that had difficultly in landing because they did not have the GPS coordinates to work with.

Mr. Schriner. A hundred miles away.

Mr. O'Bryon. Yes, a hundred miles away.

Representative Saxton. A hundred miles away?

Mr. O'Bryon. Yes. But fortunately, there was no loss of life and property. It was an incidental thing, certainly not intentional.

Representative Saxton. Mr. Kehs?

Mr. Kehs. I don't know if anybody's really done much to try to collect all of these little anecdotes.

Certainly, you know, I've personally driven too close to a television station and watched some of the electronics in the car go a little hazy.

These kinds of things happen all the time. People just sort of dismiss them, and they don't really quantify them, at least not until you get into a weapons program, and then you're looking for specific effects, and then you do begin to quantify them and you do begin to look at the statistics of when do you disrupt an airplane and when don't you.

Do you need a cellular telephone, or do you need one of Dave's devices.

I suppose we could come back to you, we could go look for some of these things a little bit. I must say, we haven't really tried to do that in the past.

Representative Saxton. Mr. Merritt?

Mr. Merritt. General Schweitzer just handed me a list that he developed to exactly this question that you have asked.

So I assume he would not mind if I passed this on. There are two pages of about 15 or so incidents.

One of the clearest, though, is also one of the oldest that he refers to, was the Forestal incident in 1967 in which a radar on board one of our carriers ignited a Zuni rocket and you may recall did tremendous damage to that carrier. Let's see, I was just looking for the number. A hundred and thirty-four officers and men were killed.

Mr. O'Bryon. Senator McCain I believe was on board that ship at that time.

Mr. Merritt. In that incident.

So, you know, that is one example where inadequate shielding was disastrous.

The same kind of thing from that level on down to just simply jamming computers are possible.

And, again, it's the kind of examples that we heard about – of turning your electronics off on board the aircraft – and also one of the clearest examples that something is going on.

There were examples of electronic disruption on aircraft and it's from these kinds of spurious signals that were not being adequately protected.

Representative Saxton. How vulnerable are our military systems since we switched the subject over to the Forestal, which is fine, I suspect that I know the answer, and it is that we are quite vulnerable.

Is that correct?

Mr. Kehs. The vulnerability of our military systems is not as casual as our civilian systems. It requires a little, having spent quite a bit of time trying to figure out how to attack military systems, in order to be militarily tactically significant, you need to have a relatively high confidence level that what you're going to do is going to be significant.

You can't wait for the GameBoy that's going to create minor problems in the airplane cockpit. You need to crank things up so that you know that you're going to create a problem.

It's a little bit more difficult.

I think that in general the military systems are probably, although vulnerable, much less at risk than the civilian systems, and that our concern at least is that there are a lot of surprises that are waiting to be discovered, as Jim, I'm sure, can give you an infinite list of surprises that have turned up in the live-fire testing.

And we stumble across those every time we go to do a test.

But for the country, I think it's the civilian systems that really need to begin to pay some attention to this, because they don't have the STARs type equivalent protection that the military builds in, even if it's intermittent and not across a broad range of military devices, the subject is getting some attention.

Mr. O'Bryon. One thing in the live-fire test program that we have established as a discipline since the very first test back in 1986 is that we require pre-shot predictions before any shot is done, whether it's a ballistic shot, a mine shot, a grenade, an RPG, a SMART weapon or a directed energy system. And we again required pre-shot predictions even for the testing that Dr. Schriner was involved with this past year.

And we continue to find that our modeling simulation is not adequate. It's just not there. We're getting better, but we have a long way to go.

And some of these models we're using are developed by the National Laboratories like Livermore, Sandia and Los Alamos and other places like that, very talented people, but it's a very complicated problem.

And the assignment is not just limited to what I'll call the circuit boards, but also the exits and the entrances and all the things getting to and from the circuit boards, what we call the "front doors" and "back doors."

So it's very complicated. I'm echoing the fact it's very difficult to predict these kinds of effects. We can guess, obviously, but it's very difficult to predict with any certainty.

Representative Saxton. Mr. Schriner?

Mr. Schriner. There are many open-source examples of this sort of thing. There's one that says that the Russian mafia has used HPM to rob banks and spring electronic locks.

Now you never know if this is true or not, but I would believe that, yes, you could do that.

And a bank is not about to let its shareholders know that it was robbed last night with something electronic. They just pay the damages and go on merrily being a banker.

So there's a lot of open source potential examples of this, but it's really hard to sort them out. It's word-of-mouth sorts of things.

Representative Saxton. Let me ask one final question.

One of the concerns that we obviously have relates to our national security, either resulting from the effect on civilian targets or effect on military targets.

Are you aware of any other countries around the world, any countries around the world that have a program to develop RF weapons that might be used in a military sense?

Mr. Schriner. Yes.

The French probably have the largest program for developing high-powered microwave systems. They have probably the largest chamber that I know of for the testing of those systems, and they regularly hold professional meetings over there where our scientists go and I think sell the candy store, so to speak, every year.

So I think the French are probably the known world leader in that. I suspect that the Chinese have very large programs also.

I've been to many professional conferences where I was appalled at the information that was just given for any taker.

One of these dish antennas, like I mentioned, was shown at the Albuquerque conference center once, on one of these professional high powered microwave programs, and there were all sorts of people out there taking pictures of that.

There was a broadcast program on the Christian Broadcast Network where they showed a microwave power gun that somebody kind of pasted together a little pistol grip with a photograph of one of those antennas from that conference.

You could talk to the scientists at these places and actually they'll tell you how to build one.

The Swedes have a fairly large program. Most countries are taking a look at this, and they would be foolish if they didn't attempt to see if they could use that for their respective purposes.

Representative Saxton. How about the Russians?

Mr. Schriner. I believe that the Russians have been the leader for a long period of time on that. I think that Dr. Merritt could speak better to that subject.

Representative Saxton. Mr. Merritt?

Mr. Merritt. I think an official answer to your question really needs to come from the INTEL community, but many countries acknowledge that they are interested in radio frequency weapons.

There being some fine distinction between interest and development.

But Russia, Sweden, France, Germany, UK, many countries, China, have expressed interest in development of RF weapons and mitigation of their effects.

Representative Saxton. Well, thank you very much.

I have no further questions at this time, and I would just like to thank each of you for being here this morning to share this information with us.

I believe the Committee has allowed the information here to be discussed to be highly classified, presented in a very objective way.

I do not believe, from what I've heard during this eight-month investigation, to conclude anything other than RF weapons constitute a credible threat to the civilian, as well as the military infrastructure of our country.

And so I have instructed my staff to make these testimonies available to the appropriate Committees.

As a matter of fact, I will be having discussions with Committee Chairmen and other Subcommittee Chairmen about our findings. It would be my strong recommendation that the appropriate resources be allocated to reduce, if not stop, the proliferation of these weapons, if that is in fact possible. At least we ought not to be intentionally providing for the proliferation of these weapons.

And that we also I think need to look at this in terms of a very serious threat to our civilian operations, as well as the military operations.

And thank you for being here today to help us make these points. We appreciate it.

(Whereupon, at 11:11 a.m., the hearing was adjourned.)

SUBMISSIONS FOR THE RECORD

PREPARED STATEMENT OF REPRESENTATIVE JIM SAXTON, CHAIRMAN

Good morning. Thank you very much, everyone, for being here.

On June 17, 1997, the Joint Economic Committee (JEC) held a hearing called, "Economic Espionage, Technology Transfers and National Security," in which it heard testimony from Lt. Gen. Robert Schweitzer about a new class of weapons, radio frequency weapons (RF), and the impact of these new weapons on the civilian and military electronic infrastructure of the United States.

Since the General talked about a terrorist threat and a proliferation threat, the JEC has continued to investigate these potential threats. I am pleased to welcome to the Committee an extremely knowledgeable group of panelists. Let me introduce them.

Mr. Alan Kehs is with U.S. Army Laboratories and will discuss the overall RF threat. Mr. Kehs has a B.S. and a M.S. in Electrical Engineering, and a M.S. and a Ph.D. in Physics from the University of Maryland. He is a recognized expert on the generation and use of intense relativistic electron beams for the production of high-power microwave radiation. Recent assignments include Chief of the Source Physics Branch and Chief of the Nuclear and High Power Microwave Technology Office. Dr. Kehs chaired the 8th national conference on HPM in April 1997 and currently chairs the tri-service HPM Technology Coordination Panel.

Mr. James O'Bryon is the Deputy Director of Operational Testing and the Director of Live Fire Testing with the Office of the Secretary of Defense at the Pentagon. He has received a B.S. in Mathematics, and he also has graduate degrees from George Washington University in Operations Research/Management Science and from MIT through the Electrical Engineering Department. The Director will discuss the role of Live Fire Testing and how it may play a role in testing our military equipment with RF weapons.

Mr. David Schriner is the Principal Engineer directed energy studies with Electronic Warfare Associates and a recently retired engineer with the naval weapons testing facility at China Lake. He has numerous patents, has received superior service awards, and given technical

presentations over 42 years of civil and military service. He will discuss the difficulty in building a RF weapon and the terrorist threat.

Dr. Ira Merritt is with the Missile Defense Space Technology Center in Huntsville, Alabama. He has more than 25 years of experience in developing advanced technologies, systems requirements, system designs, and test capabilities for ballistic missile defense systems. He has a Bachelor of Science in Chemical Engineering and advanced degrees in Nuclear Engineering. Dr. Merritt will discuss the proliferation of RF weapons primarily from the former Soviet Union.

I look forward to the enlightening testimony from our panelists.

PREPARED STATEMENT OF R. ALAN KEHS, ARMY RESEARCH LAB

Mr. Chairman and Members of the Committee, I thank you for the opportunity to help shed some light on the widely ignored topics that you have chosen for these hearings. I have spent most of the last twenty years working on various radio frequency weapons technologies and I am currently serving as chair of the tri-service High Power Microwave (HPM) technology coordination panel.

In general, our security classification guide prevents us from discussing anything but the most generic concepts and severely limits the depth of discussion if we remain at the unclassified, full public release level. It is not deemed to be in our best interests to provide details on our programs or roadmaps to weapons development that might assist rogue states, terrorists and others who would eventually wish to use these weapons against us.

However, one does not need to rely on classified reports in order to appreciate the potential impact of radio frequency weapons (RFW) or as they are frequently called, HPM weapons. Everyone in this room has undoubtedly experienced Electromagnetic Interference (EMI) to some piece of household electronics. Some common examples are the effects of lightning strikes or automotive ignition noise on radio transmission, placing two computers too close to one another on a bench, driving under power lines while trying to listen to the radio, and so forth.

A step up from these minor inconveniences is the warning that we hear each time we take off or land in an airplane. We all wonder "can a GameBoy or calculator really cause serious problems to the airplane electronics?" The answer, of course, is that a GameBoy, calculator or cellular telephone is not usually sufficient to disrupt airplane electronics, but it can happen. As a result, we adopt a policy of "better safe than sorry" and shut down electronics during the more critical take off and landing segments of commercial air flights. We have now asked the question "How much power does it take to create problems?" Realistically, these questions cannot be answered at the unclassified, full public release level. More subtly, the question becomes "At what point do common civilian electronic devices become weapons?"

Let us shift now from the low power levels (microwatts and milliwatts) of GameBoys and cellular telephones to the very high power levels (megawatts) of commercially available radar systems, TV

transmitters, and particle accelerator tubes. This is the platform from which HPM weapons programs would be based.

Conceptually, an HPM weapon looks like a radio transmitter. There is a power source, a tube to generate RF energy, and an antenna to radiate the energy appropriately. The key technologies and final products have been under development for the greater part of this century and are readily available on a broad range of markets. In the Army, we make extensive use of surplus radar and radio equipment.

Military electronics generally contain some electromagnetic shielding and protection devices -- even if they are not specifically designed to withstand an HPM attack. Commercial designers are generally concerned only with FCC limits on EMI and no one knows how susceptible commercial electronic systems might be to a concerted electronic attack. These commercial systems include our banking and telecommunications systems as well as oil and gas distribution and transportation systems, among others. Although these systems are designed to withstand the loss of a critical node, a concerted attack would cause unknown effects.

HPM technologies appear on the critical technologies list. However, the required special approvals have not slowed the transfer of increasingly powerful and sophisticated HPM technologies to overseas buyers.

The intelligence community will have to address the threat issues but I believe that they will find existing technology is more than sufficient to support several potential applications and threat scenarios.

The growing U.S. dependence on sophisticated electronics for war-fighting and domestic infrastructure makes us potentially vulnerable to electronic attack. By its nature, the Defense Department is compelled to confront such threats, however, the full range of our technological society is also at risk and much less aware of potential threats. I pray that Congress will help all of its agencies and departments to appreciate the increasing seriousness of the questions raised here today and take appropriate actions to evaluate threats and construct appropriate defensive measures.

STATEMENT BY

MR. JAMES F. O'BRYON

DEPUTY DIRECTOR, OPERATIONAL TEST AND EVALUATION
LIVE FIRE TESTING

OFFICE OF THE SECRETARY OF DEFENSE
THE PENTAGON
WASHINGTON, DC 20301

BEFORE THE

JOINT ECONOMIC COMMITTEE

DIRKSEN BUILDING, ROOM 106
FEBRUARY 25, 1998

Mr. Chairman and other distinguished members of the Committee, it's an honor for me to appear before the Joint Economic Committee today to discuss the role and mission of Live Fire Testing, and specifically as it relates to the ballistic threat, the threats posed by radio frequency and electro-magnetic pulse and other threats. As your letter of invitation states, these issues "are of great importance to our nation as well as the world."

Let me begin by acknowledging the fact that the Congress recognized, starting about a decade ago, that there was a significant and growing need to realistically test our major weapons and weapons platforms to assure that they would withstand the rigors of combat and to inflict the maximum effect on the enemy when used. The Live Fire Test legislation, first authored in Fiscal Year 1986 and strengthened several times since then, including most recently, the Federal Acquisition Streamlining Act (FASA), signed into law by the President in October 1994, requires that this realistic testing be conducted against realistic threats and that an independent report on the test results be prepared and delivered from the Secretary of Defense to the defense committees of both houses of the Congress prior to making any decision to enter full-rate production on each designated system. These systems have included armor systems, missiles, projectiles, aircraft and others. To date, literally thousands of Live Fire Tests have been conducted and evaluated and more than two dozen Live Fire Test and Evaluation reports on both weapons and platforms have been forwarded to the House and Senate in compliance with statute, prior to the decisions to enter full-rate production.

Live Fire Testing has revealed design flaws which, had they not been found in testing and corrected, would most likely have resulted in the loss of valuable equipment, and more importantly, loss of life of our combat forces. The kind of realistic testing that we require provides the opportunity to learn what otherwise would only be discovered in the first days of actual combat, and that is certainly not the time for surprises.

Since this is the Joint Economic Committee, I'm confident that your focus would be on how much this testing has cost the American taxpayer and in turn how much has been returned on these investments. I'm happy to report to you that, over the past decade since the inception of this program, although significant improvements have been made to our weapons systems as the result of this testing, not one test program has exceeded 1/3 of one percent of the program's cost. This small investment has paid significant dividends in not only military equipment saved but also savings in lives from improved combat survivability.

From its beginning, the LFT&E program has required that not only design threats be tested against our systems but that also emerging threats be tested

as well since we need to anticipate what we'll face at the end of the acquisition cycle and beyond. The System Threat Assessment Reports, or STARs, as they're known, are prepared by the Service proponents and approved by the Defense Intelligence Agency (DIA). These documents, by DoD regulation, are the primary source document used to establish what these emerging threats will be.

The threats tend to fall into three categories: classical conventional, emerging conventional threats and unconventional threats. The legislation forming the basis for LFT&E calls for testing against expected conventional threats. The Pentagon's JCS Publication 1-02 defines a conventional weapon as one which is neither nuclear, biological or chemical. Hence, testing of our chemical, biological and nuclear weapons is not under the aegis of Live Fire Testing. However, LFT&E does include other threats including directed energy threats. The focus of the STARs over the years has been on, what I term, "classical conventional threats." They have formed the basis of the DIA threat documents outlining projected threats over the years. These traditional threats are certainly the most familiar and they include such things as rockets, bullets, missiles, mines, torpedoes, grenades, shaped charges, kinetic energy penetrators, high explosives and other similar weapons which damage by depositing either kinetic energy, explosive energy or both. We have done significant testing of these threats and these threats will, most likely continue to face us well into the next century.

There is a second category of threats which, in my opinion, are of increasing importance, the directed energy threats. This category of threats includes low, medium, and high-energy lasers and high powered microwave radio frequency threats. I would like to focus the remainder of my opening statement on them.

These directed energy threats are included within the official definition of conventional threats, and hence, within the LFT&E mandate for oversight, are receiving increasing attention from the Services.

Recent defense guidance has made clear that other nations may very well choose to fight the U.S. asymmetrically, thereby avoiding a frontal assault on our forces in the more traditional war of engagement and attrition. Rather, they very well might choose to select a specific area of our potential vulnerability, for example communications, or information warfare, or other selective threat to attack us more effectively and efficiently. Recognizing that our nation, both militarily and commercially, is heavily dependent upon electronically produced, processed and transmitted information, it makes good sense to assume that rogue nations could easily try to exploit this potential niche warfare area to not only disrupt military command, control and communications but also to attempt to defeat our highly sophisticated military systems which rely increasingly on computers and their related software.

Drawing much of their technology from the commercial world, our military systems, whether they be tanks, ships or aircraft are heavily dependent upon computers or computer components. They use computers to navigate, to communicate and to acquire and home on targets. In fact, some of our new fighter aircraft literally cannot fly without their computer controls. Destroying, disrupting, corrupting or interrupting computer components could be very serious. As our computers become more and more miniaturized, faster and more proliferated, it may become feasible to attack these platforms through their potentially soft electronic components. As Mark Twain once said, "If you put all of your eggs in one basket, you'd better watch that basket."

Other technologies, such as the introduction of nonmetallic composite skins for our aircraft and armor, may, while minimizing weight, inadvertently increase vulnerabilities by eliminating the "Faraday cage" which has traditionally provided a degree of protection from external electronic disruption.

We recently initiated a series of Joint Live Fire Tests (JLF) with the three Military Departments to assess the effects of potential radio frequency weapons against our platforms. While there has been some testing of RF weapons over the years, these JLF tests were particularly interesting for several reasons: First, we were examining the survivability of our systems to such weapons. In contrast to this, most tests done previously had been to asses our lethality against potential adversaries. Second, the source was a transient electro-magnetic broadband threat, making potentially susceptible a much wider range of equipment than the more traditionally tested narrow band systems. Third, the tests were conducted outside, rather than the vast majority of other testing which has been done at short range inside enclosures. Just as one's voice sounds differently in the shower than it does outside, so does the performance of an RF weapon in the open. Fourth, the tests were done against a fully operational target, not simply a component or series of components as is often done. Just as the human body behaves as a total system, weapons platforms perform differently when tested as a complete operating system. We selected the Army's Huey Cobra Gunship as the candidate platform to gain insights into not only what the first order effects might be but also to gain insights into how to even test such systems to these threats. Our intent in testing such an older and less sophisticated platform than we are currently developing was that it would not only be less costly and more available for destructive testing but also might indicate that if such an unsophisticated platform were to be vulnerable to such threats, then our newer, more computer dependent platforms could also be. We also were able to place other devices of interest in the path of the threat with significant results.

Just three weeks ago, I and some 200 others attended a meeting in the Russell Building sponsored by the National Defense Industrial Association, at

which time the issues of information security and warfare were discussed. The act that some of our military communications are conducted over commercial lines was noted. Hence, what might first appear to be a civilian problem could also be a military problem.

Because of the rate of change of technology, in communications, computers and sensors as well as in lasers and radio frequency technology, the complexities of the issues are fast-moving.

I'm not here to imply that the sky is falling, or that our weapons don't work. What I am trying to say is that the world is changing, the potential threat is changing, and our approach to designing and testing in this emerging world must change to meet it. We must realistically Live Fire Test to these emerging threats to our military platforms and weapons. It will be a savings not only in real dollars and equipment, but in lives as well.

Thank you for your invitation to appear here this morning. I'll be happy to answer any questions you may have at this time.

STATEMENT BY
MR. DAVID SCHRINER

BEFORE THE
JOINT ECONOMIC COMMITTEE

THE DESIGN AND FABRICATION OF A DAMAGE INFLICTING RF WEAPON BY "BACK YARD" METHODS

February 25, 1998

Note, this paper reflects the personal views and opinion of the author. The material in this paper has been deemed unclassified by those who hold his security clearances but it does not specifically represent their views. This paper is a very brief statement on the subject and it is written from a non-technical point of view to provide an easy look at the subject manner by non-professional people or groups. Further elaboration on any point can be requested in either a technical format or at a classified level with the proper security restrictions in place.

For many years research activities in different countries have focused on the use of radio frequency (RF) waves as a weapon. Most of this work has been titled or described under the title of High Powered Microwave (HPM). Worldwide, large amounts of money have been invested in this technology to support both the military interests but also the industrial heating needs. Like most technologies, with maturity the applications increase and the costs to use it become lower. One primary point of this paper is that as these technologies mature they also become affordable and usable by criminals and terrorists. Most military programs are classified and the general public knows little concerning their nature but as the technology becomes available to criminals and terrorists, it may be directly applied to the infrastructure elements of our society. This paper addresses the question concerning the possibility of certain types of this technology being used against the society.

The primary focus of this paper will be on a different and new form of HPM called Transient Electromagnetic Devices (TED) that could, in the hands of enemies, criminals, pranksters, or terrorists pose a significant threat to much of the United States infrastructure components that are based on micro-circuits and computer or micro-processor control. This includes financial institutions, aircraft, security, medical, automotive, and other critical equipment used everyday in our society. The systems necessary for the production of this form of energy are much easier to construct and use than the earlier and more well known conventional HPM narrow-band systems that are currently in development for military use. Millions of dollars have been spent on the conventional HPM, systems and it is the type that DOD managers and their funding offices are well acquainted with. This paper will briefly speak to these but the main focus of it will be on the very different type, the TED systems, which is less well known and may be the RF weapon of choice to the modern cyber or infrastructure RF warrior.

Conventional HPM systems generate RF wavessimilar to those used for many different purposes including communications, heating, and radio location purposes. We are all very familiar with the term frequency as expressed in mega-hertz (MHz) when we tune our FM radios over the FM band from 88 to 108 MHz. Likewise with the AM radio band from .55 to 1.5 MHz. These expressions of frequency describe how many complete RF cycles occur each second from the radio transmitters that generate them. Radar systems also generate RF signals but these are in thousands of MHz each second (the term Giga-Hertz or GHz applies). This is the type of signal that conventional HPM systems generate or radiate, a sine wave. TED systems do not generate a sine wave and operate entirely differently than narrow-band systems.

Narrow band HPM systems are similar to microwave ovens in that they use high powered sine waves to cause material placed in their field to generate heat. This is exactly what narrow band HPM systems do, they attempt to use extremely high powered RF sine waves to cause a target system to burn out. Other types of HPM use high powered, but conventional wave-like signals to enter a target system and cause some of the conventional effects that a jammer or countermeasure system might. All of these narrow band HPM systems employ sine waves that are very different than the signals generated and radiated and employed by the TED systems.

RF power is expressed in Watts and one million Watts is expressed as "megaWatts" or MW. A kitchen microwave oven, for example. uses a magnetron tube to produce a continuous wave (CW) .5 to 1 MW RF signal to provide energy to heat the material placed in its presence. In a simple way of describing the heating, the powerful microwave signals cause the molecules of the material to rub together at the frequency generated by the magnetron and heat results in the material exposed to the field. Materials such as meat, many materials containing carbon molecules, and even water heat well when placed in such a field. Many industrial heating applications require considerably larger power levels than the home microwave oven but the basic principles are the same.

It is with this view of microwave heating that we have the first notion of the use of microwaves as a weapon. One assumes that if a microwave signal of extremely high power level is aimed at a distant target of some type. then heating and perhaps burnout of some part of the target would occur. If the signal was tuned to the operating frequency of a targeted radio receiver, for example, one would assume that if enough power was provided in the radiated beam directed at the target's radio antenna, that the radio's "front-end", that part directly connected to the antenna, could be heated sufficiently to burn it out. The key here is whether there is an entry point for the high powered signal to enter the targeted system and whether there is enough power to cause burnout.

The community involved with HPM systems generally describes a "front-door" and a "back-door" entry point. A front-door point might be, as in the above example, an antenna normally used by the target platform, such as an aircraft or a tank, for some RF function such as communication or radar. Here the RF weapon designer would attempt to radiate an RF signal into the target platform's antenna and cause either a burnout or a disruption effect. A back-door entry point might be an unshielded wire at some point on the targeted platform that would allow

the RF weapon signal to enter some part of the platform's electronic systems and, as before, cause a burnout or disruption of some sort. The weapon designer would like to have a priori knowledge of the target so as to select the right frequency and use the right modulations to accomplish the desired result.

Since this extremely high-powered RF generation technology also fills the needs of industrial heating applications, essentially very high powered microwave ovens, there is a universal worldwide need for the technology and export controls are confused when it comes to the possible use of this technology as a weapon.

The New Kid on the block, the Transient Electromagnetic Device (TED):

There is a new type of source technology currently under development in our country and, very likely, other countries as well. This type of directed RF energy is quite different than the narrow-band systems previously described. This type of directed energy is called transient electromagnetic radiation. Instead of generating a train of smooth sine-waves, as the conventional narrow-band systems do, it generates a single spike-like form of energy. This spike-like burst of potential does not have "cycles" or waves and it may be only one or two hundred pico-seconds (psec) in length. 100 psec is the time that it takes light to travel 1.2 inches and often these short time duration puoses are described in "light-inches".

It is very similar to the type of signal that occurs when you rub your feet on the carpet on a dry day and then touch your computer keyboard. An electrostatic discharge (ESD) occurs when you do this. The electrostatic charge on your body discharges onto and into the computer and a very brief amount of very high current flows quickly from your finger into the computer circuits causing a momentary break in the normal flow of signals and bits of information. Because of this momentary break in the "bit-flow" the ESD may cause the computer to crash and in some cases it may cause sensitive electronic circuits to be actually damaged to the point where they are non-functional and must be replaced. This vulnerable item may be just a single semiconductor diode in a single integrated chip in a circuit on the motherboard, and there are hundreds or thousands of these in a desk-top computer. It is often economical to simply replace a whole circuit board of components rather than trying to find the one specific circuit and replacing just it. This type of new weapon source, a transient electromagnetic device (TED), is actually a system that radiates an ESD-like signal that is intended to cause a similar responses, as just described, to the targeted system.

Let us look at the differences between narrow-band (NB) and TED HPM systems. The NB systems generate sine waves, the TEDs don't. The NB systems are very costly and go to great lengths to generate very high average powers, the TEDs don't, the NB systems are very complex systems, the TEDs are not, the NB systems generate very high average powers (microwave heating), the TEDs generate very high peak powers (and are poor RF heaters). They both use an antenna and the larger it is, the more power they can radiate, in a narrow focused beam, at the target.

In a narrow-band HPM device, high technology vacuum tubes are used that are, in some ways, very similar to those used in our highest-powered TV or FM stations and radar systems. They are very delicate devices, are complex, and very expensive. They require large amounts of primary power and generally require some type of cooling system, either air blowers or liquid types. All of this complexity requires complex engineering and development, and the manufacturing time is great and costly. Not for the amateur or a low-cost, start-up operation. Generally a highly skilled team of various technical experts of numerous engineering specialties is required to manage the development and operation of such devices.

TEDs, on the other hand, are relatively simple devices that generally use simple spark-gap switches, either in oil or in pressurized gas pulse storage lines. The power supplies are relatively small in size and much lower in average power and cost than for the NB systems. The engineering and mechanical issues are small in comparison to the narrow-band devices. The technology is well described in the various professional Pulse Power references found in good technical libraries. The significant development, engineering, and manufacturing costs are small in comparison to narrow band. Most of the technology required is available and is an outcrop of the various nuclear and flash x-ray work done in the past.

NB systems operate at some given frequency with a small bandwidth, and you will find them at one spot on the radio dial. The TEDs do not even have a definable frequency but instead, because of their short time duration, they occupy a very large spectrum space, and you will find it everywhere on every radio dial. When a TED pulse is generated it will have the ability to excite responses in systems designed to receive at any frequency from as low as 100 MHz up to several GHz, from the FM band up to the lower microwave bands. A NB system would excite only those systems that were operating at its frequency, say 2.345 GHz, so a narrow band system must be "tuned" to a given target's known soft spot but a TED system would go after any soft spot of the target platform, back-door or front door.

So what is the bottom line of this discussion?

Because of the simplicity of TED systems and the suspicion that they may cause disruptive effects to electronic systems that they are aimed at, they make an attractive approach for RF terrorists to use for various purposes. We see hints of this vulnerability in the many warnings that we get each month about locations where we should not use radios and electronic devices for fear that we will do some damage to something. They make passengers on aircraft, during take off and landing, turn off radios, games, and other electronic devices. Hospitals regularly place signs that electronic devices are not allowed. Many people do not want you using your cellular telephones near their computer. Many repair shops require that wrist-bands attached to ground be used when opening electronic equipment for repair. We have a lot of things out there in the world that either have known or suspected vulnerabilities to RF fields or electrostatic discharge. A TED system provides both of these conditions, an RF electrostatic discharge nature and its output (the number of pulses per second) can be adjusted for maximum disruptive effect. Its peak power output can be made much higher than those fields ordinarily found in everyday systems like cellular radios, radar systems, TV and FM stations, and simple ESD effects.

It clearly appears, based on testing that has been done as well the information presented at unclassified technical papers and conferences, that the TED would make a good terrorist RF weapon and that, with the proliferation of high technology infrastructure systems that are integral to everyday life in our country, we would be very vulnerable to such systems. It is also clear, because of the extreme cost of repairing all of the vulnerable systems, that until this vulnerability was shown, no one would have much concern or interest in it.

Considerable discussion and innuendo has recently been made concerning the possibility of building a TED source using "back-yard" methods, a Radio Shack Terrorist RF weapon. Such a system would have to have sufficient power to, with some degree of probability, cause detrimental effects to common infrastructure items such as those found in; financial institutions (banks, ATMs, and stores), medical facilities, airport facilities, general transportation items (auto engine controls, ABS, air-bags, etc.), utility facilities (telephone exchanges, power grid controllers), and other infrastructure entities. This type of source is imagined to be what a criminal, terrorist, or prankster could develop or build in a reasonable time, with reasonable tools and materials and with open literature or reference material.

The accomplishment of such an effort would require that either some sort of estimate of what power level would be necessary to accomplish a given objective or to simply make all of the power that could be made, and then go out and test the weapon against various target items under either controlled conditions or actual attempts against a family of established targets. Since it is an extremely complex process to even come close to some predicted level of vulnerability, using even the most advanced modeling and analysis techniques, the obvious approach would be to "go for the maximum power and then test" approach. Normal testing would be done under strict safety and security conditions but a terrorist would not have such limitations. Normal tests would be conducted at a test location but a terrorist would simply drive around the block or building until something happened.

An important criteria for an RF terrorist would be that any of the parts and materials used would have to be those that could be easily found in any city and were not traceable by conventional counter-terrorist agencies such as the local police, insurance investigators, and FBI.

It is clear that there are four basic configurations that could be used, one the size of a briefcase that could be placed very close to a target system (like a computer at a desk or counter), one that could be mounted into a small van and disguised to appear as ordinary, one that was dedicated to be set up at a remote target location and used for some purpose where appearance was not of any concern, and finally, a system that could be located in one's back yard such that it could be aimed at over flying aircraft.

The systems would likely have much in common and the builder would employ a learning curve to go to the next more advanced system. The results or vulnerabilities found with any system could be factored into the use of the next system. This learn-as-you-go process would be a natural approach for such an amateur effort.

The means of manufacturing the system includes parts and tools that one could purchase at a hardware store or those found in an average garage shop. Tools such as a small lathe with an integral milling machine (available via mail-order at a cost about $2,000), drill press, and general garage tools should be all that were needed, nothing exotic.

The effort would likely be started with the small briefcase-sized unit. It could use automobile ignition parts and a camcorder ni-cad battery for the power supply. It might use a small dish antenna bought mail-order and some parts picked up at a surplus store. The total cost of such a unit would be about $300 and it could be built in about one week. The development behind its design could be accomplished by doing some basic experiments with stun-guns or other high voltage components found in surplus stores, automotive shops, and parts from a "well equipped electronics junk box". The unit could easily be tested at close range to the type of computers and hardware found in any home office and if it caused some ill effect, then the terrorist would have proven the effectiveness of the system. Success with step 1.

The next step would be to refine the technology and increase the voltage and the repetition frequency. An advanced design might use a 6-foot TV dish antenna that could be bought mail-order (for $200) and it might use a more advanced spark-gap unit than was used in the earlier model. Such learn-as-you-go is a natural process in the design of spark-gaps.

Such a unit using a larger antenna (a mail-order 12-foot TV dish), when finished would look like a simple TV dish system and it (or many like it) could be mounted such that it could easily be pointed at over-flying aircraft.

In support of the information presented in this testimony and taking advantage of the winter's need to work indoors, a unit that uses oil spark-gaps was designed, built, and tested. The materials for it were mail-ordered at a cost of about $500 and about one week was needed to fabricate the mechanical hardware. It use two ignition coils and a battery for power, an automobile fuel pump and filter for the oil circulation, and commonly available transformer oil. An additional week was required to work out all of the electrical wiring, the oil lines, and the general finishing details. This unit was ready for testing in two weeks after starting the effort.

The signal radiated from the unit was measured and found to be a very significant power level that can be compared against available vulnerability and susceptibility levels of military equipment. When the weather permits, this unit will be tested against a set of infrastructure targets at an official test range. From the measurements and known signal levels, this unit is expected to be consistently deadly to many types of infrastructure items at ranges suitable for terrorist usage.

This quickly-developed low-cost system could easily be placed in a small van and used in a parking lot or directed at buildings that the van was driven past. It is highly likely that this type of device would be a very effective terrorist system and the findings of its design could be factored into another either a larger, higher powered device, or a more advanced design each with significantly greater effectiveness.

The net result of all of this design. experimentation. fabrication and measurement proves that such a weapon system could be made by anyone with an engineering degree or even a bright technician with good hardware experience. The technical information required can be found in open sources, if not just from good common engineering sense. The materials needed are nothing special and if the effort is made, advanced concepts can be made using everyday hardware such as automotive ignition systems. The testing to date has been very limited but the results of this testing have provided considerable insight to just what is vulnerable in infrastructure systems. This insight and work leads to a firm opinion that a terrorist would have little trouble developing such technology and that he would have a high probability of success in the use as an RF weapon against our infrastructure elements found in any city or near facilities around the country.

This work has been done within the proper security guidelines since:

1. The models made in my home laboratory/workshop used off-the-shelf materials and open-source references.

2. The laboratory tests of this hardware were made in a controlled environment with the proper security in place.

3. The results of these tests. the data capabilities, and the target set identities are kept in a facility cleared for classified storage.

4. The development of any of this hardware is reported on a regular basis to those with whom I relate at a classified level to assure that they are informed of the work and are able to apply this to their interests and efforts if necessary. Any of this hardware can be used by them for any determination of utility to military interests.

Work in this area will be continued and an aggressive test and evaluation of these "back yard" techniques and methods will be accomplished. This process will be done in cooperation, and if requested, under the direction of agencies with an interest in this non-military weapon related process. The author of this report will, if requested, provide to the Committee further details at a classified level in the proper security environment.

UNLIMITED UNDERGROUND ELECTRONICS
SUBDIVISION: KOGA-TECH WEAPONS

THIS LIST IS NOT TO BE DISTRIBUTED TO GENERAL PUBLIC WITHOUT CONSENT FROM UUE OR KOGA-TECH WEAPONS. UUE 1839-D WEST VISTA WAY #515 VISTA CA 92083.

VOICE / DATA SCRAMBLER & DESCRAMBLER UNITS. Scrambler uses digital techniques rated at 8bits and sampling of 8000hz. Descrambler uses signal recognition to unscramble the original signal. This is not a cheap noise generator, but a high tech. state of the art, high security setup. Includes two units which can scramble and descramble signals. 4" x 4" size. Includes cases w/RCA connectors. Battery or adapter powered. Can be used directly over phone lines or RF transmissions. Item #VJAM69. Cost $210.00 + $5.50s/h.

140MHZ - 180MHZ (2 METER) TRANSCEIVER. 35 watt output RF, 12 basic channels expandable. 2.2 watt audio output signal. 12vdc @ 5.6amps. 7" x 10" x 2" in case, connectors, w/mic and adapter. Perfect when used with our VJAM69 scrambler / descrambler units above. This is not the basic everyday 2 meter setup. Item #TJDR38. Cost $450.00 + $10.00s/h.

LETHAL POWER STUN GUN. Looks like a regular 200,000volt stun gun. Puts out 75kvdc @ (.5-1.25 amps of pulsed current). Extremely dangerous device for educational or high security use only. Powered by either a couple 9volt batteries or a 12V battery pack. Item #STUN1. Cost $225.00 + $6.50s/h.

HIGH GRADE PLASTIC EXPLOSIVES. Looks, feels and acts like C4 but costs about 10 times less. We will send you detailed info on how to make it and where to get materials. All materials are legal and very cheap. You can make about 20 pounds for under $140.00. This explosive exhibits fragmentive and compressive properties making it good for blowing walls down or shattering steel structures. Item #HGPE. Plans cost $12.00 + $1.00s/h.

ARMOR PEIRCING SHOTGUN SLUGS. We will show you how to make them from 4 basic materials. No chemicals or explosives used. Extremely hard 4 metal allow will not scratch bores but will peirce/cut clean holes in ¼"++ steel plates without loosing shape. We will send you the necessary tool to cut your molds into oak boards. Tool is for 12gauge only. Materials are as easy to get as going to the hardware store. Item #APSS. Plans and tool cost $40.00 + $3.00s/h.

HOUSE / BUILDING ZAPPER. This device plugs in to any wall outlet and immediately starts distorting and jamming transmissions, radio receptions, computers, and any other semiconductor device in the house or building. Powered by the wall outlet. This device may accidentally destroy semiconductor devices which are connected to the outlets. Device is totally assembled in a case and has an on/off switch. Size is about 3" x 3". Item #HBZPLAS. Cost per unit $95.00 + $5.00s/h.

UUE OR KOGA-TECH WEAPONS ARE NOT RESPONSIBLE FOR ANY LEGALITIES RELATED TO PLANS, KITS, DEVICES, PARTS OR ANY OTHER MATERIAL OBTAINED FROM UUE OR KOGA-TECH WEAPONS. YOU, THE PURCHASER, ARE SOLEY RESPONSIBLE FOR ANY USE OR MISUSE OF ANY MATERIAL OR DEVICES OBTAINED FROM UUE OR KOGA-TECH WEAPONS. ALL INFORMATION, KITS, PLANS, PARTS AND DEVICES ARE SOLD FOR EDUCATIONAL OR ENTERTAINMENT USE.

For a complete catalog send a SASE to : Unlimited Underground Electronics
1839-D West Vista Way #515
Vista CA 92083.

HIGH ENERGY ELECTROMAGNETIC RADIATION PLASMA GENERATOR.
This device is capable of generating high energy plasma radiation which can destroy semiconductors throughout a car, house, etc. Kit/plans cost $45.00 + $5.00S/H. Plans/schematic cost $5.00. Order#hplas-(kit or plans)

ULTRA HIGH ENERGY ELECTROMAGNETIC RADIATION PLASMA GENERATOR.
Over three times more energy output than above unit. This unit has a wider bandwidth of frequencies therefore has greater destructive and constructive capabilities. Plans/schematic include how to utilize this device for jamming signals and power sources and how to build a plasma antenna. Kit/plans cost $75.00 + $5.00S/H. Plans/schematic cost $7.00. Order#uhplas-(kit or plans)

MID POWER GUIDED EMP GENERATOR.
This device is similar to the one's police in LA use to stop car engines. This device utilizes two concepts for stopping a car: random frequency and magnetism. Plans/schematics cost $6.00. Order#mpemp-plans

HIGH POWER GUIDED EMP GENERATOR WEAPON.
Unlike the similar police unit for stopping cars. This unit is extremely powerful (range of over 300yds is common), similar to military weapon capabilities. This design utilizes three effective concepts: random frequency, magnetism and plasma. This device causes permanent damage to electronic devices and can also harm people. Kit/plans cost $140.00+$15.00S/H, this is a partial kit which includes the hardest parts to obtain and a 1500-3000watt emitter. (this is the main operational section needed for a working unit.) Plans/schematics cost $10.00. Order#hpemp-(kit or plans)

TUNABLE WAVE MASER WEAPON.
The military also has weapons of this nature which are capable of knocking out cities, satellites, etc. We will show you how to build a 1000-5000watt unit with extremely lethal potential. The maser beam is similar to a laser beam but operating frequency is different, so just imagine a 5000watt laser beam's capabilities. You can build one for less than $200.00 using easy to get materials. We can supply you with most of the materials needed to build one. Kit/plans cost $160.00+$15.00S/H, this is a partial kit which includes over 90% of the required materials to build this unit (kit minus tube and waveguide magnets.) you can get magnets from speakers and the tube from the hardware store. Plans/schematics cost $10.00. Order#twmaser-(kit or plans)

800-950 MHZ FREQUENCY CONVERTER.
This device will take an 800-950MHZ signal and convert it to 400-550MHZ for scanners. Plans/schematics cost $4.00 complete. ORDER#800MHZ

PROTOMAGNETIC WAVE/FIELD ACCELERATOR (REVERSE MAGNETISM).
This device forces two expanding magnetic fields together at 90 degrees, after which a scalar wave and small soliton are introduced which causes the effects. This is the same setup believed to have been used in the Philadelphia Exp...Documentation of actual philadelphia exp included. Plans/schematics cost $7.00. You must try this one. ORDER#PROTOMAG

CENTRIFUGAL GUN. THIS IS A DEVICE WHICH HAS THE CAPABILITY OF SHOOTING A BB WITH THE SAME DESTRUCTIVE POWER AS A 22 BULLET. USING A 9V BATTERY!!! PLANS/SCHEMATICS COST $5.00. ORDER#CENTGUN

RADIO WAVE RECEPTOR POWER GENERATOR. THIS DEVICE HAS THE CAPABILITY OF GENERATING POWER FROM THE RADIO SIGNALS THAT WE ARE CONSTANTLY EXPOSED TO. A LARGER DEVICE OF THIS NATURE MAY HAVE POTENTIAL TO POWER A HOUSE. PLANS/SCHEMATICS COST $5.00. ORDER#RWRPG

8-12 INCH SPARK GENERATOR. FROM 2 AA BATTERIES!!! WE SHOW YOU HOW TO BUILD IT FOR AROUND $10.00 OR LESS. PLANS/SCHEMATICS COST $3.00. ORDER#8INCH

R1 MOTOR/GENERATOR. THIS DEVICE IS SELF SUSTAINED AND THE UNIT CONTAINS THE MOTOR/GENERATOR BUILD INTO ONE UNIT. BASED AFTER MANY INGENIOUS DESIGNS INCORPORATED INTO ONE. REQUIRES NO OUTSIDE POWER SOURCE OR GAS. THIS DEVICE IS ACTUALLY BASED ON CHANGING MATTER/MAGNETISM INTO ENERGY. PLANS/SCHEMATICS COST $9.00. ORDER#R1M

R1 WATER TURBINE GENERATOR. THIS DEVICE CAN GENERATE AN ENORMOUS AMOUNT OF POWER WHEN PLACED IN LINE WITH YOUR INCOMING WATER LINE!!! IMAGINE RUNNING THE WATER AND LOWERING YOUR ELECTRIC BILL AT THE SAME TIME WITHOUT SPENDING ANY EXTRA MONEY. PLANS COST $8.00. ORDER#R1W

FULL AUTO GUN TRIGGER ATTACHMENT. THIS DEVICE IS POWERED FROM A 9V BATTERY. MAKE YOUR GUN FULL AUTO WITH ADJUSTABLE SPEED FIRE. PLANS/SCHEMATICS COST $4.00. ORDER#FULLAUTO

SOLITON WAVE GENERATOR. THIS DEVICE IS IN CURRENT TOP SECRET USE BY THE U.S. MILITARY. WE ACQUIRED THE PLANS FROM AN INSIDE SOURCE. IMAGINE AN ELECTRICAL NEUTRON BOMB, THEN THINK OF THIS DEVICE. IT IS SO SIMPLE YOU WON'T BELIEVE IT. WE KNOW THE INVENTOR AND MANUFACTURER. PLANS/SCHEMATICS COST $6.00. ORDER#SOLWAVE

TESLA EARTHQUAKE MACHINE. SIMPLIFIED. LEARN HOW TO ACTUALLY MATCH RESONANCE OF EARTH BASED STRUCTURES AND EVEN THE EARTH AND CAUSE IT TO SHAKE OR FALL OFF BALANCE. A SHOE BOX SIZED DEVICE CAN CAUSE LARGE EARTHQUAKES. PLANS/SCHEMATICS COST $7.00. ORDER#TESLAEQ

ELECTROMAGNETIC RAIL GUN. MILITARY COPIED DESIGN. THIS IS EXTREMELY SIMILAR TO THE MILITARY'S CURRENT DESIGN AND USED DEVICE. NO NEED FOR COILS!!! WE SHOW YOU HOW TO DO IT THE EASY WAY WITH LIMITED RESOURCES AND EQUIPMENT. THE MILITARY MODEL CAN SHOOT AN ALUMINUM RING AT 1/6 THE SPEED OF LIGHT. OUR MODEL CAN SHOOT AN ALUMINUM RING AROUND THE SPEED OF SOUND AND IS PORTABLE. WE WILL SHOW YOU A SIMILAR DESIGN FOR BOTH MODELS. PLANS/SCHEMATICS COST $8.00. ORDER#EMRG

PARTICLE ACCELERATING CYCLOTRON. CHANGE THE STATES OF MATTER OR GO FROM ONE ELEMENT TO ANOTHER. MAKE DEPLETED URANIUM RADIOACTIVE AGAIN. ALL WITH THIS SIMPLE TO BUILD DEVICE. IT CAN BE BUILT IN LESS THAN A DAY AND WILL COST UNDER $50.00. THINK OF IT AS AN ELECTRON ACCELERATOR. PLANS/SCHEMATICS COST $7.00. ORDER#PACYCL

WE SELL MOST OF THE PARTS NECESSARY TO BUILD MOST PROJECTS FROM OUR CATALOG. CALL US AT 760-639-5527 VM.....E-MAIL TO UUE@USA.NET OR NINTEACH@INCOM.NET.

EMF DETECTOR. WE WILL SEND YOU A TOP OF THE LINE EMF DETECTOR (WILL DETECT EMF FROM AN INDIGLO WATCH, IT'S THAT SENSITIVE) ALONG WITH INSTRUCTIONS AND INFORMATION ON EMF AND HAZARDS. ONLY $25.00 + $4.00S/H. ORDER # EMFDET

CAR ALARM DISARMER. WE WILL SEND YOU A COMPLETE KIT W/ CIRCUIT BOARD & ALL PARTS TO BUILD A SMALL POCKET SIZED DEVICE WHICH WILL DISARM ALMOST ALL CAR ALARMS. KIT $110.00 + $2.00S/H, ASSEMBLED W/O CASE $140.00 + $2.50S/H, ASSEMBLED W/ CASE $155.00 + $3.25S/H. ORDER # CARDIS-(KIT OR ASSEMBLED- W/ W/O CASE)

FEASIBLE ATOMIC BOMBS. IT IS POSSIBLE TO BUILD AN ATOMIC DEVICE WITHOUT THE USE OF PLUTONIUM OR URANIUM!!! WE WILL SHOW YOU THREE WAYS, ONE OF WHICH DOES NOT EVEN USE EXPLOSIVES, AND CAN WIPE OUT A CITY OR STATE...IF THE ENERGY CREATED COULD BE UTILIZED CORRECTLY, JUST THINK OF THE FREE POWER. PLANS/SCHEMATICS $10.00. ORDER # ATOMIC

ASTROLITE & AIG. THE MOST POWERFUL NON-NUCLEAR EXPLOSIVE MIXTURE. SIMPLE MIXTURE ONLY REQUIRES THREE CHEMICALS WHICH CAN BE BOUGHT AT AUTOMOTIVE STORES, HARDWARE STORES OR FEED STORES. ONE CHEMICAL IS OBTAINED FROM HOBBY STORES. THIS STUFF IS STRONG, REALLY STRONG - WE WERE ABLE TO DESTROY TONS OF GRANITE STONE WITH JUST A COUPLE POUNDS. (US GOV PATENTED MIXTURE) PLANS/DOCUMENTATION $5.00. ORDER # ASTROLITE

FOR KIT OR PARTS AVAILABILITY VM US AT 760-639-5527.
UNLIMITED UNDERGROUND ELECTRONICS, YOUR SOURCE.

MISSILES, We will show you how to build missiles using walmart materials. These missiles have an initial velocity of the speed of sound, yes they make a sonic boom (that can be silenced). You can build over 10 missile in under 1 hour for under $25.00. These missiles have an accurate range of over 1/2 mile. They can be aimed using a steel tube or build a sophistocated firing system. Plans/diagrams cost $6.00. ORDER#MISSILES

CALLER ID/CALL RETURN BLOCKER, Build one for under $4.00 with radio shack parts or buy the parts from anywhere. Uses around 10 parts. Will stop caller ID traces, stops call return and even slows down FBI and police traces (that's why they're trying to make them illegal). Plans/schematics cost $5.00. ORDER#CALLID

RADIO FREQUENCY / SIGNAL JAMMER, Jam, block and distort millions of frequencies with millions of bandwidths with millions of signals and data. Based on tesla technology. Illegal to build or operate under FCC regs. Used in WWII by hilter to jam radio and radar signals. Plans/schematics cost $3.00. ORDER#JAMMER

HOW TO MAKE FREE PHONECALLS, Learn the hidden art of Phreaking. Call anywhere in the world using any payphone anywhere. This simple device uses a special signal to activate the coin register or relay in payphones to make it think it is being paid. We even have a new system that works on newer phones that have no mic access. Plans/documentation cost $4.00. ORDER#PHONE

HOW TO GET FREE SODA & CASH, Soda machines hold about $25-40 in coins for change. They also hold lots of sodas. We will tell you how to get both for free using one of our devices or using store bought devices. We will send you a Radiation Plasma Generator kit (for $45.00+$5s/h) which can be used to get free soda and cash from all electronic soda machines. There is a secret spot to energize that does the trick. Plans/documentation cost $5.00. ORDER#SODA

TESLA COILS (100K, 1000K, 5000K, 10000KV), We are talking about under $300 to build a 10000000 tesla coil!!! We can supply you with all parts for any voltage or style. These plans will give you all the knowledge needed to build any of the above voltage tesla coils. We will even include plans for how to build a rotary or air adjustable spark gap unit for making a top class tuned tesla coil. Most parts can be bought from a hardware store or wire outlet. We will show you how to contain the 5000k & 10000kv models so they don't destroy themselves. Included are all necessary fomulas needed to calculate everything. Booklet cost $10.00. ORDER#TESCOIL

HOW TO ERASE YOU FINGER-PRINTS, We will send you detailed info that depicts 3 methods to erase your finger prints temporarily. From 1 day to as long as 1 month. Simple methods can be used at anytime and will erase prints and stops oils or cells from your fingers from getting on anything. These methods are used by the FBI and other agencies around the world. We are not talking about putting gloves on but high tech material. Plans/docs cost $3.00. ORDER#PRINTS

HOW TO MAKE A 1HZ TO 3GIG FREQ COUNTER, These plans will show you step by step, part by part what to use to make a top class 1hz at 60mhz res counter. Costs about 30.00 to make one. Size is around 4x4x1 1/2". Complete plans/schematics cost $5.00. ORDER#COUNTER

HOW FUEL CELLS WORK AND HOW TO MAKE ONE, We will send you info so you can understand how they work and how to build your own hydrogen or acid/alcohol fuel cell. These are the things used on the space shuttle for power. They can also be used in conjuction with cold fussion to convert the h2 and o2 to electricity. Plans/docs cost $5.00. ORDER#FUELCELL

ANY OF THE FOLLOWING PLANS COST ONLY $1.00 WITH ANY NORMAL PLANS PURCHASE!!!!!!!!

1. HOW TO MAKE CS TEAR GAS USING GLYCERINE AND ???. ORDER#CSGAS
2. HOW TO MAKE OS TEAR GAS USING NH4 AND ???. ORDER#OSGAS
3. HOW TO SCREW OVER SOMEONE WHO PISSED YOU OFF REALLY BAD. ORDER#PISSOFF

BULK ITEMS FOR SALE AT ALL TIMES..

1. (13.2% PEPPER + CS TEAR GAS) CANS POLICE SIZE UNITS (4OZ) 10 FOR ONLY $95.00
2. 75000 VOLT STUN GUNS (VERY SMALL BUT STRONG) 5 FOR ONLY $120.00
3. LOCK PICK SET (CUSTOM) (RAKE, TOGGLE & TURNER) 5 SETS ONLY $40.00
4. POLICE HANDCUFFS (DOUBLE LOCKING REAL THING, INC 2 KEYS EACH) 5 FOR ONLY $75.00

ADD $10.00 S/H FOR EACH BULK ITEM BOUGHT.

LYSERGIC ACID / LSD. LEARN HOW TO MAKE IT WITHOUT USING TONS OF EXPENSIVE CHEMICALS. LYSERGIC ACID IS NATURAL AND EASY TO MAKE IN JUST A FEW DAYS. WE WILL SHOW YOU HOW TO MAKE IT, WHERE TO GET MATERIALS (SUPERMARKET) AND HOW TO USE IT. PLANS/DOCUMENTATION $4.00. ORDER # LSD

#8, J1, COMPOUND DETONATORS. WE WILL SHOW YOU HOW TO MAKE DETONATORS FOR USE IN HIGH EXPLOSIVE MIXTURES. WE WILL TEACH YOU STEP BY STEP HOW TO MAKE DETONATORS THAT ARE COMPARABLE TO MILITARY TYPES. THESE ARE REQUIRED TO SET OFF REAL EXPLOSIVES. MATERIALS ARE EXTREMELY EASY TO GET ANYWHERE. PLANS/DOC'S $5.00. ORDER # DETS

SOLID STATE MATRIX DISPLAY O-SCOPE. Make a dual trace 20MHZ led matrix display o-scope for dirt cheap. This unit is in current use by us in our labs. It is simple, cheap, accurate and portable. Plans include board layout, parts list, etc. Kit includes all parts and perf board. Plans cost $6.00, kit cost $85.00 + $3.00s/h. Every part can be bought from JAMECO. You will be surprised by the quality circuit design and effectiveness of this model. ORDER#SSMDOS

12VDC TO 115AC INVERTER. BUILD ONE FOR LESS THAN $15.00. We will show you how to make one with just 10 components. no joke. Make one with true sin wave signal at over 100watts. Easy design is used by many manufacturers to make em fast and cheap, they sell for around $49.00 in stores. Plans cost just $3.00. ORDER#12VINV

WHITE / PINK NOISE GENERATOR. This device will distort bugs, taps, wires, recorders, video taps, etc... We will show you how to connect one to your phone line for the maximum in safety. Tap detectors only tell you if your tapped, what can you do—you can attach a white / pink noise generator. Generates white / pink, digital / analog, random 33 bit signals. Plans show how to power it from the phone line or a 9 volt battery. Plans cost $5.00, kit cost $35.00 + $2.00s/h complete with circuit board and manual. ORDER#WPNG (KIT OR PLANS)

GARAGE DOOR CODE FINDER. Just push the button and within minutes the garage door opens. Design is simple and works on over 80% of the current electric garage doors on the market. Plans cost only $5.00. ORDER#GDCF

MERCURY VAPOR ION LASER. We changed a 2mW HeNe laser tube into a 10watt mercury vapor ion laser using our newest plans. These plans will show you step by step how to build a Hg vapor ion laser using easy to get materials from tons of sources. This laser puts out two wavelengths: 567.7nm green and 615nm red which can be split using a prism. Plans cost $6.00. Order #hglaser.

COMPUTER VIRUSES. We will send you a disk which has 12 of the nastiest viruses on it. These are legal because they have renamed extensions which can easily be renamed in dos by you. Some include: casino virus, aids, sub zero, redx, etc. To be used for testing anti-virus programs only. Disk only $11.00. S/H free. For an extra $5.00 we will include 10 additional viruses. Order # virus (10 or 20)

COMPUTER VIRUS MAKER PROGRAMS. We will send you a disk which has two virus maker programs which will enable you to make over 50 viruses and set their parameters according to who they will attack. Even make them undetectable and uncleanable. Disk only $15.00. S/H free. For an extra $5.00 we will include 10 viruses. Order # vmaker (program or program+10)

COLD FUSSION. We have never to this day offered our R1 cold fussion cell in plan form. We feel we must in order to spread this growing field and offer the world a free, clean source for unlimited energy. We developed our own cell using catalytic converter parts and other easy to get materials. You can build one for about $150.00 that is powerful enough to run a car or small house. This design uses three concepts instead of only two like most cells out there, heat, hydrogen and pressure. We designed it to be optimum in all three areas. It really puts out more than is put in, a lot more. Plans/schematics cost $10.00. ORDER#COLDR1

TRACKING / HOMING DEVICE. We will show you how to build one using already available materials for less than $45.00. Has a range of over two miles and signal field strength meter. Xmtr can run for weeks on just one charge. Operates in a frequency band that is hard to scan because of interference. Plans/schematics cost $5.00. ORDER#TRACK

RADIO-FREQUENCY JAMMER

FREE GIFT TO PREFERRED CUSTOMERS

DISCLAIMER: IT IS A VIOLATION OF FCC RULES AND REGULATIONS TO BUILD AND USE THIS DEVICE.

THE CONCEPT OF THIS DEVICE IS BASED AFTER A SPARK GAP OSCILLATOR. A HIGH VOLTAGE TRANSFORMER SUPPLIES POWER TO THE L/C TUNED CIRCUIT WHICH IS TUNED TO A VARIATION OF THE FREQUENCY OR FREQUENCIES YOU WANT TO JAM. IN OTHER WORDS, TUNE IT TO WITHIN A FEW 100KHZ OF THE FREQUENCIES YOU WANT TO JAM. THIS DEVICE WILL GENERATE AN EXTREMELY WIDE BANDWIDTH AT A VARIATION OF FREQUENCIES. A LARGE PORTION OF THE RADIO FREQUENCY SPECTRUM IS COVERED BY THIS DEVICE, AM, FM, SSB, SW, ETC. BE CAREFUL WHEN USING HIGH VOLTAGE.

THEORY: C1 CHARGES TO NEAR THE INPUT VOLTAGE AND CAUSES A SPARK TO BE GENERATED BETWEEN THE SPARK GAP. THIS COMPLETES THE CIRCUIT THROUGH L1 AND C1. L1 CREATES A CEMF OR INDUCTIVE KICK WHICH DOES THE SECOND HALF OF THE WORK. THIS DEVICE CAN PUT OUT AN EQUIVELENT OF AROUND 75WATTS IF POWERED BY OUR ULTRA HIGH ENERGY ELECTROMAGNETIC RADIATION PLASMA GENERATOR, KIT IS ONLY $75.00+$3.00S/H. THE SECONDARY INDUCTOR PICKS UP THE MAGNETIC FIELDS GENERATED BY L1 AND TRANSMITS THE ENERGY VERY EFFECTIVELY.

PARTS:

1X 110VAC POWER CORD AND SWITCH.
1X 5000-30,000VAC OUTPUT TRANSFORMER @ BETWEEN 10-60mA CURRENT.
1X VARIABLE SPARK GAP....SEE FIGURE 1.
1X HIGH VOLTAGE CAPACITOR RATED 2X INPUT VOLTAGE. (WHEN USING THE BELOW EQUATIONS TO FIND RESONANCE OR THE FREQUENCY YOU MUST USE THE uF OF THE CAPACITOR....IN OTHER WORDS THE FREQUENCY WILL DETERMINE YOUR uF OF THE CAP AND mH OF THE INDUCTORS.)
1X SET OR VARIABLE TUNED INDUCTOR, L1.
1X SET OR VARIABLE TUNED INDUCTOR, L2.
1X ½" DIAMETER COPPER TUBING OR PIPE FOR ANTENNA.

FORMULAS YOU MIGHT USE.

$Xc = \frac{1}{(6.283)(F)C}$ $\quad Xl = (6.283)(F)L$ $\quad$ FULL WAVE ANTENNA LENGTH 938/FREQUENCY IN MHZ

VALUES YOU MIGHT WANT TO USE.

C1= .01uF @ 2X INPUT VOLTAGE.
L1= COIL OF MAGNET WIRE #16 @ 1 INCH DIAMETER X 1 INCH LONG (NO GAPS BETWEEN WIRE)
L2= COIL OF MAGNET WIRE #16 @ 1 INCH DIAMETER X ½ INCH LONG (NO GAPS BETWEEN WIRE) YOU CAN PLACE THIS ON OR NEXT TO L1.
ANTENNA= USE A 6-12 INCH LENGTH.

SCHEMATIC DIAGRAM.

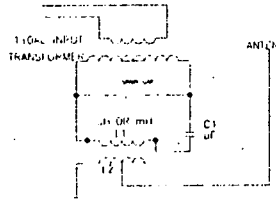
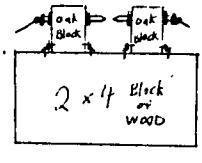


Fig 1



Rev 03

HIGH POWER GUIDED EMP GENERATOR WEAPON

WE ARE NOT LIABLE FOR ANY ACTIONS, OUTCOMES, DAMAGES, HARM, DEATH, ETC FROM CONSTRUCTION, OR EXPERIMENTATION OF THIS DEVICE. DO NOT BUILD IT!!!

THANKS TO TESLA AND SOME OTHER GREAT ENGINEERS FOR THE CONCEPTS AND THEORY BEHIND THIS INGENIOUS DESIGN. CAUTION MUST BE USED WITH THIS DEVICE, IT IS CAPABLE OF KNOCKING AIRPLANES OUT THE SKY, DESTROYING SATELLITES AND EVEN HARMING OR KILLING PEOPLE. IF YOU BUILD AND USE THIS DEVICE YOU WILL BE SUBJECT TO ALL LIABILITY FROM IT. THIS DEVICE CAN TURN OFF AND DESTROY ELECTRONIC AND ORGANIC MATERIALS. DO NOT AIM AT PEOPLE OR PROPERTY.

THE RANGE: AROUND 300-500YDS.
THE CONCEPT: BASED ON TESLA DESIGN AND CONCEPTS OF MAGNETIC VORTEX FIELDS. TESLA KNEW THAT MAGNETIC FIELDS MUST COLLAPSE, BUT HOW THEY COLLAPSE MAKES ALL THE DIFFERENCE IN THE WORLD. UPON ENERGIZING THE PRIMARY COIL, IT ACTS AS BOTH AN ANTENNA AND A FIELD GENERATOR. IT ENERGIZES THE SECONDARY COIL WITH A GREATER FIELD AND AS A WHOLE ACTS AS AN AMPLIFIER FOR THE VARIED FREQUENCIES GENERATED THROUGH THE ARC GAP AND RESONANCE OF THE COILS. ITS VERY HARD TO UNDERSTAND BUT DO SOME HOMEWORK AND YOU WILL. THE THIRD CONCEPT UTILIZES MICROWAVE RADIATION-I DON'T THINK I HAVE TO EXPLAIN MICROWAVE RADIATION CAPABILITIES. JUST PUT A WALKMAN IN THE MICROWAVE AND TURN IT ON, I THINK YOU CAN CONCIEVE WHAT WOULD HAPPEN.

FOR INFORMATION ONLY!! DO NOT USE THIS DEVICE FOR DESTRUCTIVE PURPOSES!!!

PARTS LIST:

HARDWARE

PIPE1	1	40 INCH LONG ALUMINUM PIPE W/ 3 INCH DIAMETER
TAPE	ROLL	CLOTH TAPE.
PAINT	CAN	ONE CAN OF EPOXY PAINT, HV INSULATION.
GLUE	TWO TYPES	HIGH TEMP SILICON, HIGH TEMP EPOXY.
1/16" steel plate	1 (3.15" DIAMETER)	THIS MUST BE POLISHED ON ONE SIDE.

ELECTRICAL

TRAN1	1	20,000-30,000 V TRANSFORMER AC OUT.
RSPK	1	ROTARY SPARK GAP. FIG 1.
WIRE1	ROLL	16 GUAGE FOR HARNESSING.
WIRE2	ROLL	22 GUAGE FOR SECONDARY.
CAPS	1 EACH	.0001pF 250KVDC & .1uF 60KVDC (CALL US LEAVE MESSAGE)
TUBING	4FT	1/4" COPPER TUBING FROM HARDWARE STORE.
MAG1	1	1200 WATT MAGNETRON.
MPOW1	1 UNIT	1200 WATT POWER SUPPLY.
SWITCH	1	HIGH POWER TOGGLE SWITCH.

WE ARE NOT LIABLE FOR ANY DAMAGES, HARM, DEATH, ACCIDENTS, ETC CAUSED BY CONSTRUCTION, USE OR EXPERIMENTATION OF THIS DEVICE OR DEVICES SIMILAR TO IT.

CONNECTION OF MAGNETRON TO TUBE.

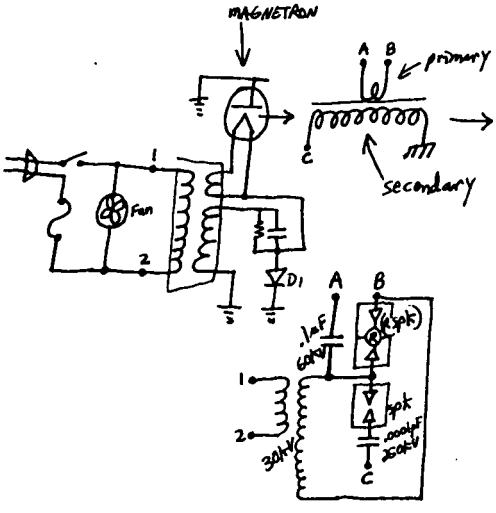
THIS IS A DANGEROUS TASK....IF IT IS NOT DONE CORRECTLY IT COULD BE CATASTROPHIC.

BEFORE CONNECTING THE MAGNETRON, YOU MUST DRILL A 2 INCH HOLE IN THE SIDE OF THE PIPE ABOUT 5 INCHES FROM THE END. THE END IS WHERE THE STEEL PLATE IS TO BE PLACED. IT MUST BE FASTENED DOWN AND GROUNDED ALONG WITH THE PIPE. THE BEST MATERIAL TO USE TO FASTEN THE MAGNETRON TO THE ALUMINUM TUBE IS SCREW TIE DOWNS. THE MAGNETRON MUST BE IN DIRECT CONTACT WITH THE ALUMINUM TUBE. THE TUBE ACTS AS A WAVE GUIDE FOR THE MICROWAVE RADIATION.

THE NIPPLE PROTRUDING FROM THE FRONT OF THE MAGNETRON MUST BE IN THE ALUMINUM TUBE'S SIDE. YOU MUST FASTEN THE MAGNETRON TO THE TUBE. THE NIPPLE IS THE OUTPUT PORTION OF THE MAGNETRON. THE BEAM OF MICROWAVES COMES OUT OF THIS PART. MAKE SURE THE WINGS ON THE MAGNETRON ARE PERPENDICULAR TO THE TUBE, NOT PARALLEL. YOU MUST FIND A WAY TO CONNECT THE MAG TO THE TUBE AND STILL KEEP THEM PERPENDICULAR.

IT IS VERY IMPORTANT THAT YOU SOMEHOW CONNECT A COOLING FAN ONTO THE MAGNETRON. IT WILL BURN OUT IF YOU DO NOT COOL IT. ALSO PLACE SHIELDING AROUND THE MAGNETRON/POWER SUPPLY AFTER YOU INSTALL IT. THE SHIELDING SHOULD COVER THE ENTIRE MAGNETRON AND POWER SUPPLY. PLACE ALUMINUM FOIL ON THE FAN BLADES ALSO. COVER EVERY OPENING WITH ALUMINUM TAPE.

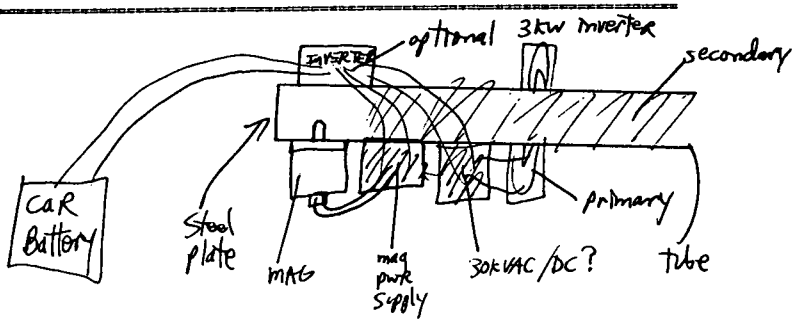
DETAILED SCHEMATIC

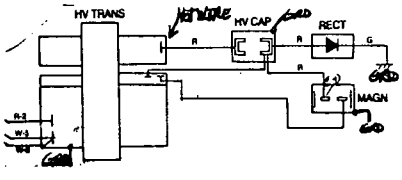


= Tube Ground

= Earth Ground

PICTORAL DIAGRAM OF FINAL DEVICE.





Magnetron to PWR Supply Hook up Diagram.

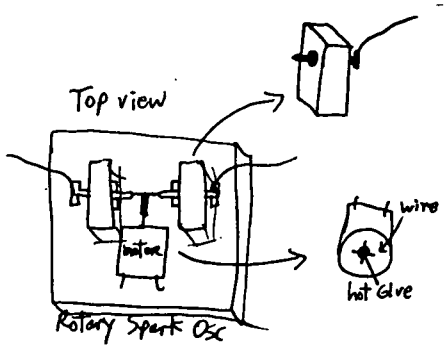
HOOK THE SPARK GAP UP TO THE COIL AND THE POWER SUPPLY. THIS WILL CAUSE RANDOM FREQUENCY TO BE GENERATED THROUGH THE TUBE AND HELP MODULATE THE MICROWAVES WITH THE SIGNAL.

WE ARE NOT LIABLE FOR ANY DAMAGES, DEATH, HARM, DESTRUCTION, USE OR MISUSE OF THIS DEVICE OR DEVICES LIKE IT. THE USER OF THE DEVICE IS SOLEY LIABLE FOR ALL ACTIONS AND OUTCOMES PERFORMED WITH THE DEVICE.

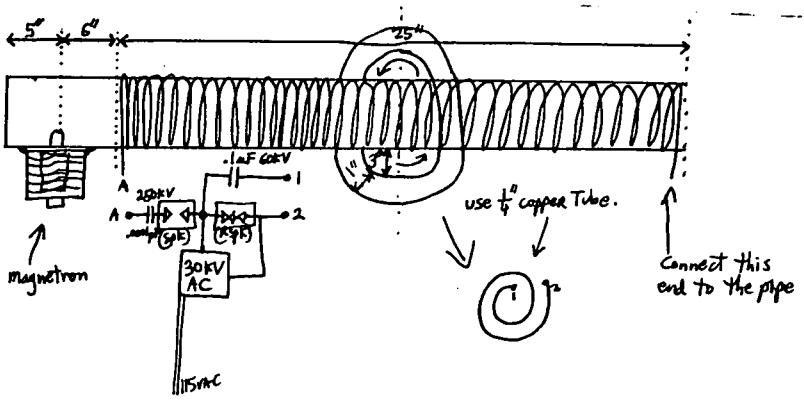
FIG 1.....SPARK GAP CONTRUCTION...

PARTS NEEDED:

TWO 1/4 INCH NUTS AND BOLTS.
2X4 WOOD...4INCHES LONG.
12 GA WIRE FOR HARNESSING.
MOTOR WITH ROTOR, PLASTIC.
HOT GLUE GUN



WRAP 25 INCHES OF WIRE (FLAT AND LEVEL NOT BUNCHED UP) ON THE PIPE, IT MUST 6 INCHES FROM THE MAGNETRON.



UNLIMITED UNDERGROUND ELECTRONICS

ORDERING FORM DATE OF ORDER:_____

NAME:_____PHONE:_____

MAILING ADDRESS:_____

CITY:_____STATE:_____ZIP:_____

ORDER#	DESCRIPTION OF ITEM	QTY	SHIPPING	COST

SHIPPING TOTAL_____

METHOD OF PAYMENT (CHECK ONE)

MERCHANDISE TOTAL_____

O CHECK
O MONEY ORDER

TOTAL ENCLOSED_____

CANADIAN/FOREIGN ORDERS MUST EMAIL US FOR SHIPPING FEES BEFORE ORDERING. NINTEACH@INCOM.NET.

MAKE CHECKS OR MONEY ORDERS PAYABLE TO:

UNLIMITED UNDERGROUND ELECTRONICS
1839-D WEST VISTA WAY #515
VISTA CA 92083

VOICEMAIL #:
760-639-5527 (24HRS)

YOU MUST BE 18 YEARS OF AGE TO ORDER KITS OR DANGEROUS WEAPONS.
BY SIGNING BELOW YOU UNDERSTAND THE ABOVE STATEMENT AND ALL DISCLAIMERS.

SIGN:_____DATE OF BIRTH:_____

SPECIAL KITS OR DEVICES/LASER STUFF FOR SALE AT ALL TIMES...

1. **FM (BELOW AND BEYOND THE 88-108MHZ RANGE) RF AMPLIFIER KIT.** TWO UNITS THAT ARE POWER CONNECTED TO GIVE A 6 MILE RANGE. DEVICE COULD BE MADE AS SMALL AS A MARTINI OLIVE AND POWERED FROM A WATCH CELL FOR DAYS. KIT/INSTRUCTIONS (ALL PARTS SUPPLIED) COST $45.00 + $2.50S/H. ORDER#FMAMPKIT

2. **RUBY LASER RESONATOR MIRRORS (FRONT AND BACK).** WE FINALLY HAVE THEM, AS MANY AS YOU NEED. UP TO 100 WATTS CAPABLE THAT WE KNOW OF. FRONT IS 80-90% MIRRORED AND THE BACK IS 97.5-99.9% MIRRORED. VERY HIGH QUALITY WITH QUARTS & STEEL CONSTRUCTION FOR MAXIMUM IN HEAT DISSIPATION. SOLD AS A SET (FRONT AND BACK) COST $35.00 + $2.50S/H. ORDER#RESONATORS

3. **MINI-SOLITON/EMP EMITTER.** THIS KIT HAS THE POWER SUPPLY, BATTERY HOLDER, ALL PARTS, AND A MOBIUS ANTENNA WHICH CAN ALSO BE USED TO TRANSMIT SCALAR WAVES THROUGH SPACE. RANGES MAY VARY: EMP 0-12", SOLITON 0-24", SCALAR 0-INFINITY. DANGEROUS VOLTAGES MUST USE CAUTION. SIMILAR DEVICES ARE USED TO CHEAT ELECTRONIC GAMBLING MACHINES. COST $75.00 + $3.50S/H. MUST BE 18 TO ORDER. ORDER#MINIEMP

4. **RECHARGEABLE 12VDC BATTERY PACK.** USED IN MANY OF OUR DEVICES. $20.00 + $2.50S/H. ORDER#12VPACK

5. **RECHARGEABLE 15VDC BATTERY PACK.** USED IN MANY OF OUR DEVICES. $20.00 + $2.50S/H. ORDER#15VPACK

6. **HIGH POWER LASER DIODES.** POTENTIAL FOR CUTTING WOOD, SOLDERING, WELDING, WEAPONS, ETC...900nm w/200ns pw. TWO UNITS AVAILABLE: 15WATT (ITEM#15WLD) COST $110.00. 75WATT (ITEM#75WLD) COST $240.00. ADD $6.50S/H FOR EACH ONE ORDERED.

SPECIAL DEAL ON OUR NEW 1 MILE PHONE BUG KIT. EASY TO BUILD, CAN BE MADE AS SMALL AS AN OLIVE, POWERED BY LINE, PICKUP ON FM RADIO... COMPLETE KIT W/INST COST ONLY $8.00 + $1.00S/H. ORDER#PHONEBUG

BUY ANY FIVE PLANS AND TAKE OFF $5.00 FROM TOTAL. BUY ANY 10 PLANS AND TAKE OFF $8.00 FROM TOTAL. ANY ORDER OVER $300 CAN CHOOSE FIVE FREE PLANS.

ALL PLANS ARE SHIPPED FREE WITHIN 1-3 WEEKS UNLESS STATED OTHERWISE.
ALL KITS, PARTS OR ASSEMBLIES ARE SHIPPED WITHIN 1-6 WEEKS.
PLANS AND PARTS ARE NON-REFUNDABLE. UNATTEMPTED KITS OR ASSEMBLIES ARE SUBJECT TO A 30% RESTOCKING FEE UNLESS OTHERWISE STATED.

MAKE CHECKS/MO'S TO: ***UNLIMITED UNDERGROUND ELECTRONICS***
MAIL ORDERS TO: ***1839-D WEST VISTA WAY #515***
VISTA CA 92083

THANK YOU FOR YOUR ORDER. OUR RESEARCH DEPENDS ON YOU.

BOOKS FOR SALE:

1. KOGA NINJITSU (THROWS/TAKEDOWNS, VITAL STRIKES) AN INTRODUCTION TO KOGA NINJITSU'S VAST ART OF TAIJITSU BY MASTER RHOADES. 55PGS PAPER BACK. HIGHLY ILLUSTRATED PICTURES. COST $12.00 EACH. ADD $2.00 S/H. ORDER#NINBOOK

2. KOGA NINJITSU (KUJI KIRI MEDITATION) AN OVERVIEW OF WHAT STUDENTS IN OUR DOJO LEARN ABOUT THE JUMON HAND SYMBOLS. BY MASTER RHOADES. STUDENT BOOKLET. ILLUSTRATED PICTURES. COST $5.00 EACH. ADD $1.50 S/H. ORDER#JUMON.

Unlimited Underground Electronics

PARTS AND ONE TIME BUYS FOR SALE, FIRST COME FIRST SERVE

1 RUBY LASER POWER SUPPLIES. We have ONE LEFT. Item #Ruby1 has an input of 115vac and output voltage of 600volts. Power up to a 800 watts. It has either steady or pulsed capabilities and can flash at rates of 0-60 fps. Very nice units from naval medical facility. Cost: Ruby1 is only $275.00+15s/h. We will send you a 100watt ruby rod with your purchase of any ruby power supply.

1 ULTRAVIOLET HEATER TUBE. We think it is an ultraviolet laser tube, but can't tell. We have no specs or paperwork. Made by berkin elmer coleman mst. Div...cat#55-0505 made in england. We think it takes 1000vdc with a element current of 12volts@1.2amps. Came out of medical equipment from a Naval hospital. Cost is $15.00~$5.00s/h.

3 HEWELET PACKARD LASER MODULES. These laser printer modules came out of large HP laserjet printers. We have three. Each module contains many mirrors, fiber optics, stepper motor with power supply, lenses, a nice IR laser diode and many other goodies. Item #Hplasermod. Only $15.00ea+3s/h.

25 RADIATION SENSITIVE PHOTOMULTIPLIER TUBES. These super high gain tubes came out of an x-ray radiation metering and monitoring device. These tubes are one of a kind. They only requires 4 wires to operate. These can be used to build a laser bounce listening device or maybe even a geiger counter. Item #Phototube. Special price: $5.00EACH MINIMUM 5. We have 25 left. .50 EA S/H

LARGE BUNDLES OF DEVICES, PARTS & PROTOTYPES. We do a lot of research and development here at UUE. We always have lots of spare parts and sub assemblies left over. Occasionally we gather it all up and sell it cheap. This bundle includes: circuit boards loaded with gold chips and connectors, power supplies, big capacitors, laser modules, coils, transformers, magnets, motors, broken ruby rods and much much more. We estimate this bundle to be worth at least $300.00min. We are selling it for only $50.00+$20shipping. It is heavy. NEW STUFF EVERYDAY.

WE ALSO HAVE: OXYGEN/CO2 METERS X3 $25EA+$10S/H, MEDICAL EVAPORATORS X2 $20.00+$10S/H, MILITARY DYNAMOTOR (28V INPUT, 1000V OUTPUT) X1 $30.00+$20S/H, MEDICAL CENTIFUGE X1 $30.00+6S/H, [X, Y, TTL MONITORING O-SCOPE] X1 $25.00+10S/H, ??? LASER POWER SUPPLY TRANSFORMER (115 INPUT, 12KV OUTPUT @ 60MA) X1 $45.00+25S/H.

NEW SHIPMENT... MILITARY RUBY RODS. All rods are 1/8 inch diameter AND flattened on each end.
4-5 inch ONLY 8 LEFT $20ea. 5-7 inch ONLY 12 LEFT $30ea. 8-10 inch ONLY 12 LEFT $50ea. Add $2.00 per rod.

WE HAVE LASER RESONATOR MIRRORS FOR SALE, HUNDREDS OF THEM. FRONT AND BACK MIRRORS WHICH WERE TESTED TO UP TO 100WATTS PULSED AND 50WATTS CONT...$35.00+2.50S/H PER SET. ORDER#RESONATORS.

WE HAVE R1 GENERATOR COIL ASSEMBLIES FOR SALE!!! WE HAVE TWO. CONSISTS OF A HUGE COIL, MANY MAGNETS AND A MOTOR. 9V INPUT GIVES A 10,000V OUTPUT. COST $40.00. 9V INPUT GIVES A 400V OUTPUT. COST $30.00. ADD $10.00S/H FOR EACH ONE.

WE HAVE THE CAPACITOR BANK AND HIGH POWER SWITCH FOR SALE!!!THIS IS OUR RESEARCH BANK. 400VDC @ .25f THIS IS VERY POWERFUL. WE WERE ABLE TO SHOOT ONE POUND STEEL SLUGS AT OVER 900FPS, STRAIGHT THROUGH STEEL PLATES. WITH THIS CAP BANK AND SWITCH. BANK INCLUDES ALL HARNESSING WIRE AND SAFETY GEAR. BUY IT AND WE'LL THROW IN A SMALL COIL. CLEARANCE COST $120.00 + $20S/H.
ADD ANOTHER $75.00 AND WE'LL THROW IN THE CHARGING UNIT WHICH CONSISTS OF A LARGE TRANSFORMER AND A HIGH POWER RECTIFIER DIODE WHICH WILL CHARGE THE BANK IN UNDER ABOUT 30 SECONDS. FOR A TOTAL OF ONLY $215.00. FIRST COME FIRST SERVE

IF YOUR MERCHANDISE TOTAL IS OVER $300.00 YOU CAN CHOOSE FIVE PLANS FOR FREE.
(PLEASE ALLOW 1 TO 6 WEEKS FOR PARTS DELIVERY) ALL ITEMS SHIPPED FREE UNLESS STATED.

MAKE CHECKS PAYABLE TO: UNLIMITED UNDERGROUND ELECTRONICS
1839-D WEST VISTA WAY #515
VISTA CA 92083

OR SEND US E-MAIL TO: Nimrod@ncom.net OR VOICEMAIL TO: 619-903-3991 (ORDER QUESTIONS ONLY) FOR LIABILITY WE MAKE NO CLAIMS THAT ANY PARTS, PLANS/SCHEMATIC, OR KIT C AN, MAY OR WILL PERFORM WHAT IS NOTED IN ANY UUE DOCUMENTATION OR ADS

PREPARED STATEMENT

Supporting Invited Testimony To Be Presented By

Dr. Ira W. Merritt*

On

Proliferation and Significance of Radio Frequency Weapons Technology

Before The

Joint Economic Committee
10:00 AM, 25 February 1998
Dirksen Senate Office Building

Chief, Concepts Identification and Applications Analysis Division
Advanced Technology Directorate, Missile Defense and Space Technology Center
U. S. Army Space and Missile Defense Command

INTRODUCTION

Thank you for your invitation and for this opportunity to offer testimony to the Joint Economic Committee regarding the proliferation of radio frequency (RF) weapons technology and its significance to the operability of our high value assets. I am employed by the U.S. Army Space and Missile Defense Command, but some of the opinions and conclusions expressed are based upon my own past experiences and observations and are not necessarily those of the Army.

I am from the Advanced Technology Directorate (ATD) of the Missile Defense and Space Technology Center, U.S. Army Space and Missile Defense Command. One of our principal responsibilities is to develop innovative and advanced technologies for application to Army projects, joint missile defense projects and other programs of national importance. In particular, ATD evaluates the capabilities of technologies, including radio frequency weapon technologies, to establish their significance to the operability of our sophisticated electronics. Our interest in RF weapon technologies has increased in the last several years as a result of:

- Rapid advances in RF sources and antennas
- Increased interest by other countries, and groups, in RF weapons and RF mitigation
- Increased susceptibility to microwaves of miniature solid state electronics
- Insights from our travel to Russia and from ongoing technical exchanges with Former Soviet Union scientists and co-workers in United Kingdom, Sweden, and Australia.

Our work with Russian scientists has been particularly useful in confirming that their approaches to technical problems are often very different from ours. Over the past several years we have visited laboratories developing directed energy weapon technologies, pulsed power systems, high power microwave technologies, high power lasers, and space-based neutral particle beams. In 1992, we visited the Moscow Radio Technical Institute, which was developing high-power microwave (HPM) sources and which had a large test facility for performing susceptibility and effects measurements. In 1994, we visited the Kharkov Physico-Technical Institute in Ukraine, where they were developing: high power microwave sources, such as the magnetically insulated linear oscillator (MILO); neutral particle beam sources; prime power systems; and where they were also performing susceptibility and effects tests. The MILO was invented in the U.S., but we discontinued work on it in the late 1980s. The Soviet Union (SU) picked up the technology and successfully continued its development. Russia also exploited the magnetocumulative generator (MCG) as an explosively driven power supply. The MCG was developed by Dr. Andrei Sakharov in the SU and the Russians have used MCG power supplies extensively to drive ultra wideband (UWB) and HPM sources, lasers, and railguns. In 1995 we visited: the Kurchatov Institute to discuss laser and high current problems, the All-Russian Electrotechnical Institute to discuss high voltage technology, Ioffe Physico-Technical Institute in St. Petersburg to discuss ultra fast switches, and the Institute of Problems of Electrophysics, also in St. Petersburg, to discuss pulse power and plasma technologies. My comments in the rest of this testimony are based upon the results of visits to Russian laboratories, visits to other countries, continued scientific contacts, research reports from contracts, some test results and open source literature.

BACKGROUND

History: It has long been a concern in the scientific community that Soviet scientists led the world in development of RF weapon technologies. This concern was heightened in 1994 when Gen. Loborev, Director of the Central Institute of Physics and Technology in Moscow, distributed a landmark paper at the EUROEM Conference in Bordeaux, France. In this paper Dr. A. B. Prishchepenko, the Russian inventor of a family of compact explosive driven RF munitions, described how RF munitions might be used against a variety of targets including land mines, sea skimming missiles, and communications systems[1,2,3]. He further popularized these munitions with articles in Russian naval journals and in other professional journals and magazines[4].

The Soviet Union had a large and diverse RF weapons program and remnants of this work continue today within FSU countries. The scope and results of the Soviet program are poorly understood, but ATD personnel have been at the forefront of efforts to gather information and to understand it[5] and its accomplishments through Windows on Science and contracts for R&D effort. Our principal objective is to understand requirements and to identify technologies applicable for RF mitigation. Nevertheless, large uncertainties still exist concerning the status of RF weapon development and associated efforts to mitigate their effects on electronics. In spite of these uncertainties, it is clear that many nations continue to aggressively pursue the development of RF weapons and techniques to mitigate their effects[6].

Proliferation: Worldwide interest in RF weapons has increased dramatically in the last several years. The collapse of the Soviet Union is probably the most significant factor contributing to this increase in attention and concern about proliferation. A recent study of open source literature dealing with RF weapons[6] clearly documented the worldwide interest in RF weapon technologies and my testimony is offered in the context of these conclusions. A few of the report's key judgments were that:

1) "...construction of effective explosively-driven Flux Compression Generator devices is entirely feasible for established military powers such as Russia, China, France, Germany, et cetera,..."

2) "There is no confirmed evidence of employment of such a device to date ... available in open sources".

3) "Modern Metal Oxide Semiconductor technology, on which most of our critical national infrastructures depend, unless deliberately protected or "hardened", is extremely vulnerable to even low–power electromagnetic pulses..."

4) "...it is well understood that the US is disproportionately more vulnerable to RF attack than are less developed nations."

Specific examples of interest in RF weapons and the proliferation of this technology follow. The French Gramat Research Center has dedicated significant assets to study the effects of electromagnetic energy on electronics and in 1989 Thompson CSF published brochures in which they stated that they were developing RF weapons[7]. A 21 January, 1998 newspaper article in the Swedish newspaper SVESNSKA DAGBLADET[8] reported that the Swedish National Defense Research Institute purchased a Russian "suitcase bomb" that uses high power microwaves to "knock out" computers and destroy all electronics within the radius of its "detonation". The

article also reported that this device is being sold commercially and that it has been sold to the Australian military. The price was reported to be several hundred thousand Kroner, or about $100,000. Mr. Carlo Kopp, an Australian professor, who claims to have had a relationship with their military, has his own web site (http://www.cs.monash.edu.au/~carlo) and has provided detailed papers on the alleged effects of RF weapons and sketches of design concepts[9]. A simple search on the Internet recently identified 95 websites that referenced Mr. Kopp's work. These included 16 sites in the U.S. and 18 sites in other countries, not including Australia. The Internet is becoming a significant factor in enhancing the interest in RF weapons.

Waveforms and Susceptibility: State of the art semiconductors are becoming more vulnerable to the effects of radio frequency energy as semiconductor features become smaller and smaller[10,11,12]. Commercial microelectronics make heavy use of metal oxide semiconductor devices which fail when subjected to voltages that exceed the dielectric strength of the component or when the device melts as a result of heating from currents induced by the RF pulse.

High-power microwave and ultra wideband signals differ in their pulse length and frequency content (Figure 1). HPM sources produce short, very high power, narrowband pulses, often billions of watts (gigawatts) in billionths of a second (nanoseconds). If HPM waveforms are in-band, they can efficiently couple energy into the target and energy is available to disrupt or to cause damage to sensitive "front door" components that are connected to antennas. However if the HPM frequency is not in-band, the energy must enter through a "back door" and coupling to the target is generally poor. In this case, much less energy enters the target to disrupt or to cause damage. UWB sources generate a much wider band of frequencies than do HPM sources, and thus ensure that some energy is at a frequency to efficiently couple to the target. However, since the energy is spread across a wider band, the power spectral density is lower and the amount of energy available in a waveband is also much lower. As a result, an UWB device is more likely to disrupt than to destroy a target, except at very close range. Many UWB sources can be repetitively pulsed and therefore can continue to disrupt the target as long as the source is functioning and within effective range. Many systems tend to be susceptible to disruption or damage at specific, sometimes unpredictable, frequencies. As a result, UWB weapons are well suited to exploit these susceptibilities, since they produce significant energy over a wide range of frequencies. This area has been aggressively researched by the Soviet Union, Russia, and others.

Extensive work has been conducted to understand the effects of high-altitude nuclear EMP (HEMP) on systems and components, but these data are mostly for frequencies less than 1 GHz and for pulse widths in the range from 50 nsec to 1usec. The shorter pulses characteristic of HPM and UWB waveforms are significant because current methods for protecting electronics from HEMP, and other anticipated sources of disruption, will not be effective against pulses from RF weapons. High-altitude nuclear EMP does not have significant energy above a few tens of megahertz, whereas HPM spectra are typically in the few gigahertz to tens of gigahertz range and UWB spectra may contain energy in the frequency range from hundreds of megahertz to a few gigahertz. There is extensive information on the effects of lightning and nuclear EMP on electronic devices, but these pulses are significantly longer than the pulses from HPM and UWB sources. Since HPM and UWB pulses tend to be shorter than the response times of most limiters, their RF energy can pass largely unattenuated into the target and cause upset or damage before

the limiter can turn on. Tests over the last 10 years have produced data on component responses to pulse widths in the range from 1 to 50 nsec. However little information is available that describes electronic responses for incident pulses having sub-nanosecond pulsewidths. Testing is needed to establish effects of the following general waveforms: very short (nanosecond and sub-nanosecond) single pulses, multiple closely-spaced very-short pulses, and long (millisecond) pulses.

Much of the existing effects data is from direct drive tests. Such tests produce the most repeatable indication of whether or not the pulse in question will upset or damage the device being tested. However these tests do not help clarify the issue of whether or not the RF waveform in question will actually couple through the walls, openings, filters, cables, and wires that separate components at risk from the external environment. This uncertainty creates a situation in which even the best analysis must be based upon significant assumptions. As a result, our commercial and military systems may be much more, or much less, susceptible to upset or damage than we now assume. As a result, characterization of representative components and circuits and the effects of physical configurations are badly needed for very short pulses.

A 1996 paper by Bludov, et al[12] from the Kharkov Physico-Technical Institute, Ukraine described HPM and UWB testing on electronic components and biological systems. The paper identified three levels of damage: temporary upset, permanent upset, and burnout. It appears that Ukraine has a systematic program to characterize the effects of HPM and UWB waveforms on electronic components.

EXAMPLE WEAPON RELATED TECHNOLOGIES

RF weapon-related sources can be classified in several ways, including: HPM or UWB, pulsed or continuous, single shot or repetitively pulsed, and very short pulse (nanosecond) or long pulse (microsecond to millisecond). In addition, the electrical or explosive power source has a significant effect on the output characteristics of the device. For example, the explosive driven munitions described by Mr. Carlo Kopp and the RF munitions described by Dr. Prishchepenko are single shot devices that convert the chemical energy of high explosives first into magnetic energy, then into electrical energy and finally into microwave energy. This multi-step conversion of energy is inherently inefficient, but explosives are very compact sources of energy, modern electronics are not very robust to external sources of energy, and the intent is to place the source/weapon as close to the target as possible. Electrically driven devices have fewer energy conversion steps, but typically they are larger and produce less power per pulse.

Electrically Driven Devices: The electrically driven (non-explosive) devices require an external power supply and energy storage system, which often leads to larger and less self-contained systems than can be produced by explosive-driven approaches. However, two recent technologies that minimize this limitation are the solid state pulsers developed at Ioffe Physico-Technical Institute in St. Petersburg and the RADAN system. These devices are quite compact and can be powered by small hand-carried energy sources.

Pulsers developed at Ioffe Physico-Technical Institute are based upon very fast (nanosecond and picosecond) solid state "on" and "off" switches developed by Prof. Igor Grekhov and Dr.

Alexi Kardo-Syssoev. These switches have recently been used to generate 10 nanosecond, 10 KHz pulses for a prototype ground penetrating sensor that is now being used commercially in St. Petersburg (Figure 2). This 10 kg portable sensor is said to be used routinely to image to depths of 200 meters with an accuracy of 1% of the depth and it is claimed to be able to image down to 1000 meters with slightly lower resolution[13]. Jammers based upon these switches can be made small enough to fit into a briefcase. A recent version is said to weigh 6.5 kg and to deliver fields of 30 kV per meter at 5 meters. This is comparable to high-altitude EMP (HEMP) field strength. An optimized version is said to deliver 100 kV per meter at 5 meters[14,15] and the pulse width and repetition rate can be tuned to have the maximum effect on the intended target.

RADAN[16] (Figure 3) is a compact high-current electron accelerator that is a little smaller than an attaché case and weighs about 8 kg with its rechargeable 12 volt battery power supply, but not including its antenna. RADAN can be used to stimulate several outputs including lasers, x-rays, wide band RF and high power microwaves that allow RADAN to be used as a jammer. RADAN output parameters are: total output power > 5 MW; repetition rate up to 1 kilohertz; pulse width about 2 nanoseconds; and output pulse bandwidth from 1 MHz to 5 GHz. A directional antenna has been developed and the developer has proposed that RADAN could be used to stop car engines and to destroy the electronic arming and firing circuits of bombs. Limited testing of RADAN has been conducted in the U.S. and it was found to affect calculators and electronic watches.

The Russian built NAGIRA radar produces short powerful pulses with the following characteristics[17]: 10 GHz fixed frequency, 5 nanosecond pulse length, 300 MW peak power, 2 Joules per pulse, 150 Hz pulse repetition rate. NAGIRA was purchased by the UK Ministry of Defence and was delivered to Defence Research and Evaluation Agency (DERA) Frazer, near Portsmouth, in November 1995. Indications are that the UK will use NAGIRA to investigate detection of fast moving targets in sea clutter, to study electromagnetic–pulse penetration into equipment and to measure the effectiveness of front-end protection devices. During initial field trials near Nizhny Novgorod, Russia (Figure 4), NAGIRA was able to track a helicopter at more than 150 km range and at altitudes as low as 50 meters. We understand that because of electromagnetic interference (EMI) concerns, Russian helicopters were not allowed to operate within several miles of the radar when it was operating at full power.

Explosively Driven Devices: Compact explosive-driven radio frequency munitions (Figure 5) being developed by Russia have recently received a great deal of attention. These munitions are claimed to range in size from a hand grenade to a 155-mm artillery shell[18] and the output may be either a HPM or an UWB pulse. Since these warheads are part of a projectile, they are intended to detonate very near their target, so fratricide is not a problem as it would be with HEMP.

In June 1997, a U.S. measurements team led by the Advanced Technology Directorate participated in a joint series of measurements on radio frequency munitions (RFM) at a site near Nalchik, Russia[5]. The purpose of these tests was to verify Russian claims about the output of Dr. Prishchepenko's compact explosively-driven RFM. The test results left Russian claims unconfirmed, since most U.S. measurement equipment was not allowed by Russian authorities to reach the test site and since Dr. Prishchepenko's team claimed that the RFM that were tested radiated in a band that could not be measured with equipment at the site.

ATD engineers continue to evaluate RF weapon technologies, to work closely with other countries, and to identify technologies that can be adopted for military applications and commercialization. We maintain relationships with other scientists through direct personal contact at conferences and site visits, through small research contracts, in collaboration with the U.S. Department of State on International Science and Technology Center (ISTC) and Science and Technology Center of the Ukraine (STCU) projects, and through the U.S. Air Force's Windows on Science Program. ATD has been extremely effective in identifying and executing joint projects, such as the joint radio frequency munitions test in Russia and briefings on the solid state pulsers developed at the Ioffe Institute in St. Petersburg. We are now working to bring the underground imaging sensor and its developers to the U.S. to test its ability to detect land mines. Solid state switches developed by the Ioffe Institute are now imported by a U.S. company that produces water purification equipment using Russian pulse power hardware. ATD has cooperated in hosting many scientists under the Windows on Science Program, including a scientist from Loughborough University in England, the only university that designs, tests, produces and markets inexpensive MCGs.

Many source and antenna technologies can be used to produce devices with very different output characteristics. For example, Russia reports that its cylindrical shock wave source generates a single gigawatt pulse about a nanosecond long. However, susceptibility tests in the FSU and U.S. suggest that irradiating a target with a train of nanosecond pulses is more damaging than a single pulse, since multiple pulses lower the damage threshold of the target[12]. As a result, Russian emphasis has been on devices that produce a train of pulses. Some designs are said to generate 50 to 100 pulses, each about a nanosecond long, in a burst of pulses about 10 microseconds long[18].

The implications of this summary are that there is an increasing variety of equipment capable of generating very short RF pulses that are capable of disrupting sophisticated electronics. These pulses are not addressed by current design standards and will challenge existing front-end RF protection and other forms of EMI protection. New capabilities are needed to reject high-power, very-fast RF pulses and to minimize their effects on systems.

We believe that common EMI and EMP mitigation techniques will not provide adequate protection against nanosecond and sub-nanosecond pulses from future radio frequency weapons, since active mitigation device response times are typically several nanoseconds to microseconds. Faster solid-state devices do not now have the high power capability needed to protect systems from RFW pulses.

RF RISK MANAGEMENT

Several fundamental questions must be answered before we can adequately understand the potential risk that radio frequency weapons pose to our military forces and civilian infrastructure. These questions are:

"What are the current and expected capabilities of RF weapon technologies?"

"What are the effects of these weapons on potential targets?" and

"What is the likelihood that our systems will be exposed to RF weapons as a result of terrorism, conventional conflict, etc.?"

As I have stated, Advanced Technology Directorate has initiated high payoff research and development efforts to understand RF weapons technologies and we have also begun to develop broadly applicable RF mitigation techniques that can ensure the operability of our high-value assets in the presence of stressing electronic warfare environments. Our emphasis is on development of near-term, low-cost capabilities that are applicable to a broad range of military and commercial-off-the-shelf (COTS) electronics and that are relatively insensitive to the details of RF weapon output. We are achieving success in this effort and believe that superior results can be obtained by selectively involving a relatively small number of highly innovative and skilled researchers and that this can be done without a great commitment of funds. For example, one of our recent $100,000 research efforts provided test results that demonstrated the ability of a low-temperature sinterable liquid to reduce external RF fields by many orders of magnitude over a frequency range from a few megahertz to a few gigahertz. This low-cost material has broad military and commercial applications. It will greatly enhance our ability to use COTS electronics on the digital battlefield and to protect key elements of the national infrastructure.

In my opinion, a more comprehensive risk mitigation effort should include the following tasks:

- **Characterize expected electromagnetic environments by analyzing and understanding rapidly advancing RF source and antenna technologies.** A variety of RF sources have been identified that could be used in RF weapons and that produce environments that can challenge the operability of our systems. We should evaluate these technologies, assess their potential for weaponization, and provide information to guide hardening measures required to mitigate their effects. The results of this task should be:
  1) credible information on the output of electrically-driven and explosively-driven RF sources;
  2) much better understanding of the capability of the rest of the world to threaten the performance of our sophisticated electronic systems,
  3) much stronger technical basis on which to develop broadly effective and low-cost RF countermeasures.

- **Conduct tests to determine the effects of short pulse RF waveforms on representative electronic components, subsystems and systems.** This task should establish the effects of anticipated radio frequency weapon waveforms on representative circuits to provide a basis for development of mitigation techniques for COTS and military electronics. It should test representative electronic circuits to RF weapon-like waveforms in a laboratory environment to better predict the coupling of RF energy into targets and to measure the effects on targets. The targets characterized should consist of representative classes of COTS and military electronics, i.e. commercial Global Positioning System (GPS) receivers, radios, computers, satellite communication systems, components from tactical operations centers (TOCs), etc. This effort should leverage ongoing Defense Special Weapons Agency (DSWA) EMP and HPM mitigation activities, which address a part of this problem, and should jointly select synergistic items for testing. This will permit unique insights into the robustness of

representative electronics to all types of RF disturbances. The target electronics should be tested in anechoic chambers available at several service facilities and should use appropriate RF sources to ensure repeatable waveforms at the appropriate power levels and with appropriate frequency content. The target electronics should be instrumented so that both the effects of the radiation and the method of coupling can be determined. These results will permit quantification of the specific performance/capability needed for each mitigation technique.

- **Use the results of effects tests to develop front-end limiters and electromagnetic interference (EMI) shields.** This task should develop and quantify mitigation capabilities and implementation guidelines for low-cost, low insertion loss, miniature plasma limiters and low-cost, very light-weight films, filters, and software algorithms to reduce internal and external electromagnetic interference produced by either local/friendly emissions or high power hostile emissions. Since RF warfare and EMI spectra cover such a broad range of frequencies and power levels, several mitigation techniques will be required.
  - Traditional methods of EMI isolation often use metal enclosures to prevent unwanted radiation from entering the circuit. These shields provides effective protection, but they add weight and are not applicable to some newer systems that may use COTS with lightweight, nonmetallic enclosures that provide little or no EMI protection. Low-cost, light-weight RF isolation techniques are needed that can be cheaply applied to COTS and military equipment to significantly increase their ability to continuously operate on the electronic battlefield.
  - Analyses are now being performed on miniature plasma limiter front-end protection devices that are compatible with solid state manufacturing processes. Analysis will confirm the feasibility of a low-loss miniature plasma limiter and its essential parameters such as threshold electric fields, gas breakdown and recombination times. This device is intended to be installed in front of sensitive antenna and receiver elements to protect them from damage or disruption by incident high power RF signals.

CONCLUSIONS

We cannot now precisely quantify the risk presented by radio frequency weapons, but we know that the risk is growing. I believe that we can respond to this risk by developing near-term, low-cost, broadly-applicable mitigation techniques. These techniques can greatly reduce our susceptibility to radio frequency weapon environments and thereby reduce the risk to our technological superiority that is essential to our military and economic preeminence.

I again thank the Committee for the opportunity to appear and to comment on the proliferation of radio frequency weapons and their significance to our critical infrastructures.

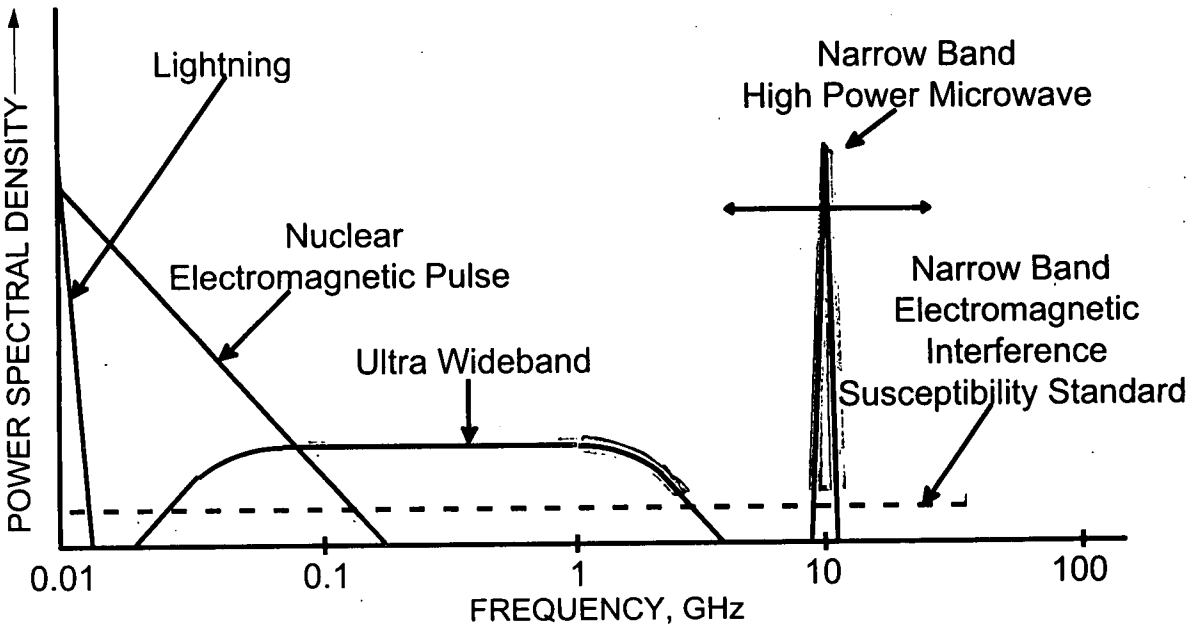
ACRONYMS

ATD	Advanced Technology Directorate
CSWS	Cylindrical Shock Wave Source
COTS	Commercial Off-The-Shelf
DSWA	Defense Special Weapons Agency
EMI	Electromagnetic Interference
EMP	Electromagnetic Pulse
FCC	Federal Communication Commission
FSU	Former Soviet Union
GHz	Gigahertz
GPS	Global Positioning System
GW	Gigawatt
HEMP	High Altitude EMP
HPM	High Power Microwave
ISTC	International Science and Technology Center
kV	Kilovolt
MCG	Magnetocumulative Generator
MHz	Megahertz
MILO	Magnetically Insulated Linear Oscillator
MW	Megawatt
NNEMP	Non-Nuclear EMP
RF	Radio Frequency
RFM	Radio Frequency Munition
STCU	Science and Technology Center Ukraine
SU	Soviet Union
TOC	Tactical Operations Center
UWB	Ultra Wide Band

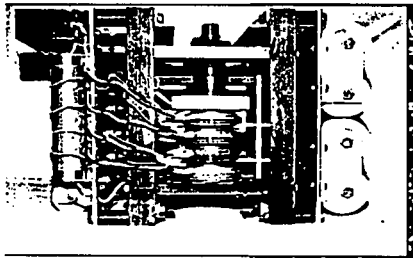
REFERENCES

1. Prishchepenko, A.B., V.K. Kiseljov, and I.S. Kudimov. "Radio Frequency Weapon at the Future Battlefield", Proceedings of the EUROEM Conference, Bordeaux, France, June 1994.
2. Prishchepenko, A.B. and V.P. Zhitnikov. "EM Weapon (EMW) in Air Defense or Some Aspects of Application of EM Radiation in the High-Frequency Band as a Striking Force",
3. Prishchepenko, A.B. and M.G. Akhmetov. "Radioelectronic Strikes in General Forces Operations (Combat)", Voyennaya Mysl', No. 2, March-April 1995, pp. 42-48.
4. Prishchepenko, A.B. "Electromagnetic Munitions", 96UM0427, Soldat Udachi, Moscow, No. 3, 1996, pp. 45-46.
5. Altgilbers, L.L., I. Merritt, M. Brown, J. Henderson, D. Holder, and Merriwhether. OCONUS Radio Frequency Munitions Test Report, ATD-98-001, 4 December 1998.
6. Linder, J.C., W.R. Graham, M.S. Hewitt, and T.J. Skucas. Radio Frequency, Electromagnetic Pulse, and High-Power Microwave Weapons, National Security Research, Contract No. N39986-97-M-7241, 18 August 1997.
7. Lucien, Vayssie, Communications and Public Relations Supervisor, Centre d'Etudes de Gramat, Gramat, France.
8. Stockholm Daily SVESNSKA DAGBLADET, 21 Jan 1998
9. Kopp, C. "The E-Bomb: A Weapon of Electrical Mass Destruction", http://www.infowar.com/mil_c4i/mil_c4i8.html-ssi.
10. Taylor, C.D. and D.V. Giri. High Power Microwave Systems and Effects, Taylor and Francis Pub., 1994.
11. Benford, J. and J. Swegle. High Power Microwaves, Artech House, 1992.
12. Bludov, S.B., N.P. Gadetskii, K.A. Kravtsov, Yu. F. Lonin, I.I. Magda, S.I. Naisteter, E.A. Prasol, Yu.V. Prokopenko, S.S. Pushkarev, Yu.V. Tkach, I.F. Kharchenko, and V.I. Chemakov. "Generation of High-Power Ultrashort Microwave Pulses and Their Effect on Electronic Devices", Plasma Physic Reports, Vol. 20, No. 8, 1994, pp. 643-647.
13. Personal Communication with Moose Hill Enterprises, 22 January 1998.
14. Grekhov, "Semiconductor Switches and Generators of Gigawatt-Range Micro- and Nanosecond Pulses", 14th IEEE International Pulse Power Conference, Baltimore, MD, June-July, 1997.
15. Kardo-Sysoev, A.F., S.V.Zazulin, V.M. Efanov, Y.S. Lilkov, and A.F. Kriklenko. "High Repetition Frequency Power Nanosecond Pulse Generation", 14th IEEE International Pulse Power Conference, Baltimore, MD, June-July, 1997.
16. Yalandin, M.I., G.T. Smirnov, V.G. Shpak, and S.A. Shunailov. "High-Power Repetitive Millimeter Range Back-Wave Oscillators with Nanosecond Relativistic Electron Beam", Proceedings of the 11th International Conference on High Power Particle Beams, Vol. 2, Prague, 1996, pp.388-391.
17. Bunkin, B.V., A.V. Gaponov-Grekhov, A.S. Eltchaninov, F.Ya. Zagulov, S.D. Korovin, G.A. Mesyats, M.L. Osipov, E.A. Otlivantchik, M.I. Petelin, A.M. Prokhorov, V.V. Rostov, A.P. Saraev, I.P. Sisakyan, A.V. Smorgonsky, and V.A. Suvorov. "Nanosecond Radar System Based on Repetitive Pulsed Relativistic BWO", Proceedings of the 9th International Conference on High-Power Particle Beams, Washington, DC, May 1992, pp. 195-202.
18. Prishchepenko, A.B. and V.P. Zhitnikov. "Microwave Ammunitions: SUMM CRIQUE", Proceedings of the AMREM Conference, Albuquerque, NM, May 1996, in publication.

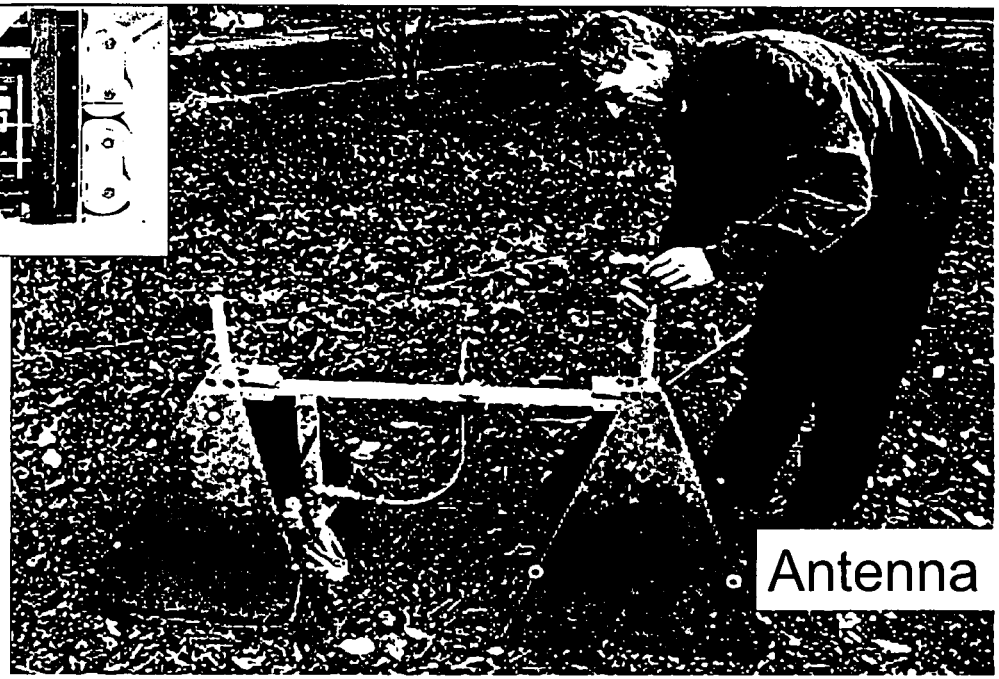
RELATIONSHIP OF ELECTROMAGNETIC SOURCES



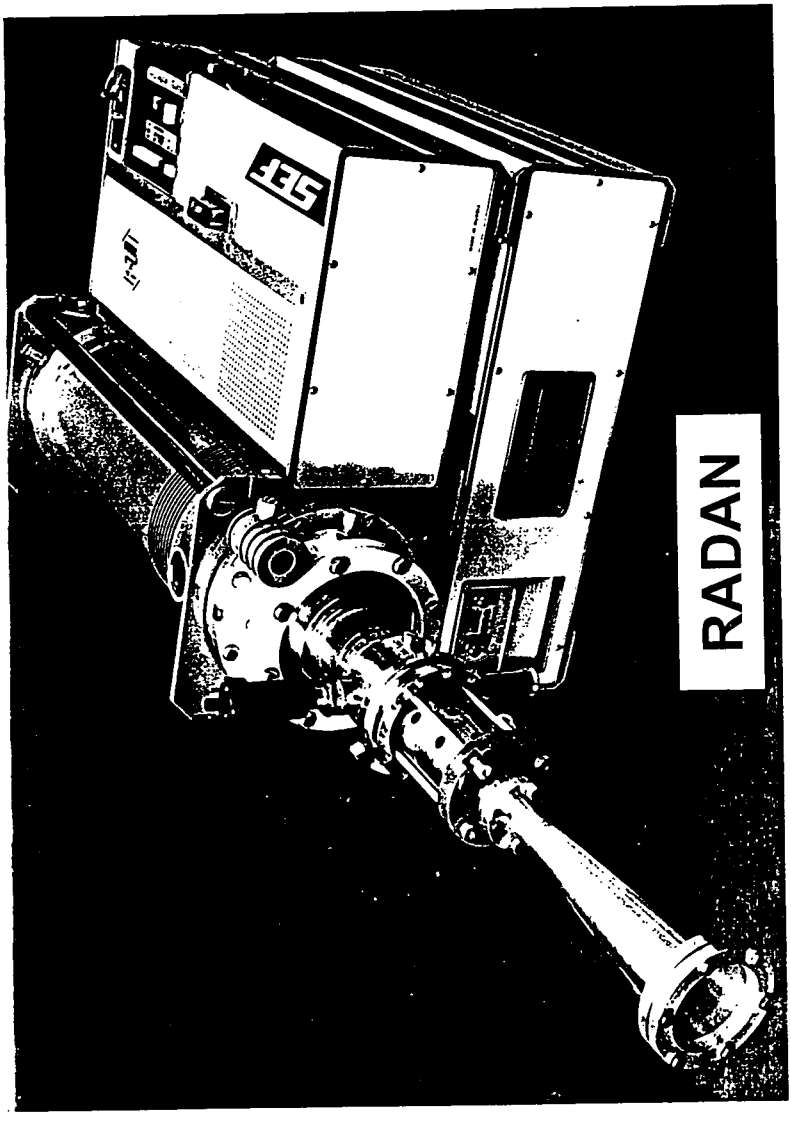
IOFFE PULSER



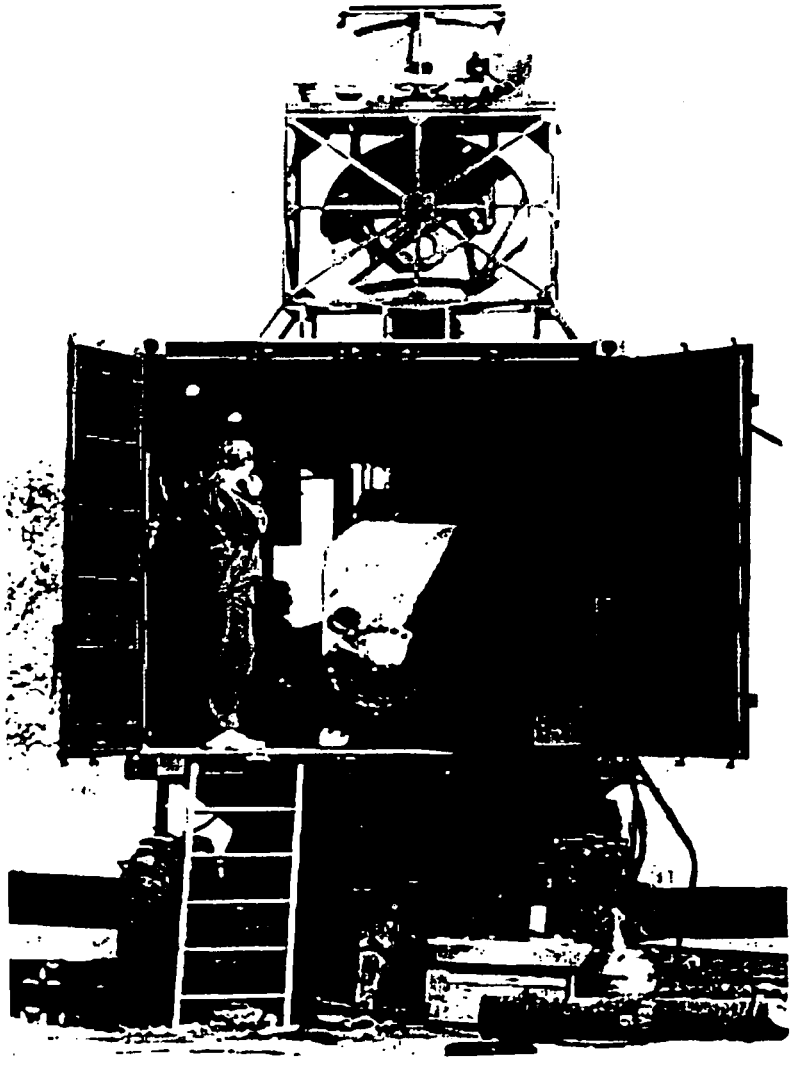
Pulser

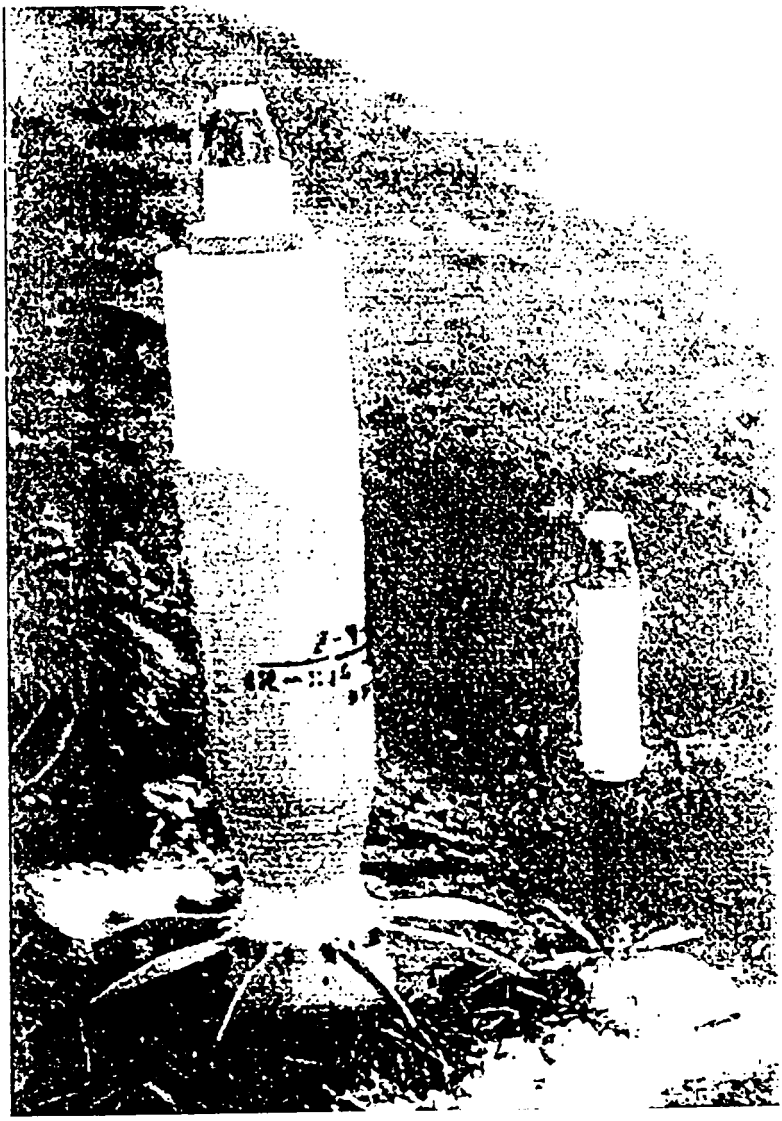


Antenna


RADAN

NAGIRA RADAR





EXPLOSIVE-DRIVEN RFM

SAINT-PETERSBURG, RUSSIA

IV.PRODUCTS

Typical parameters of the company's units are shown in the following table:

model	output voltage at 50 Ohm load	rise time	pulse width	avr.PRF (burst PRF)	power supply	special feature	size (mm)	time of delive-ry in monthS
NPG-80	>80KV (at 100 Ohm load)	<0.7ns	1-2 ns decay	1KHz	+300DC	Oil cooled	300*300*150 main block 300*300*150 heat exchanger	6
NPG-20	>20 kV	<0.7 ns	1-2 ns decay	1 kHz	+5,+100, +0-300VDC		300*200*120	2
NPG-10N	>10 kV	1-2 ns	5-10 ns decay	1 kHz	+50, +900-1800VDC	matched with non-ohmic load	70*50*30	2
NPG-10-100	>10kV	0.6ns	1ns decay	100KHz	+200 V DC		300*200*120	3
NPG-10-25	>10kV	0.6ns	1ns decay	25KHz	+200 V DC		200*140*100	3
NPG-30	>30kV	<0.7ns	1-2ns decay	1.5kHz	+28,+300VDC		300*200*120	3
NPG-30P	>30 kV	< 4 ns	20 ns	3 kHz	300-500VDC or 220/380VAC	avr. output power>1.5 kW	300*200*200 heat exchanger	4
PPG-20	>20 kV	<100ps	1.5 ns decay	1 kHz	110/220 VAC		300*230*120	2
PPG-10-25	>10K	<100ps	1ns decay	25KHz	+200 V DC		200*140*100	3
PPG-2	>2 kV	<50 ps	1-2 ns decay	10 kHz (200kHz)	5,27,200VDC or 110/220VAC		300*200*120	2
PPG-2d	>2 kV	<100ps	0.1-1ns decay	200 Hz	+5,+1000VDC	trig.delay <30ns	50*50*30	2
PPG-2S	>2 kV	<100ps	.01-10 ms step	1 kHz	+10,+100VDC		50*50*30	2
PPG-2SV	>2 kV	<100ps	10-100 ns flat top	1 kHz	+10,+100 VDC	fall time <5 ns	50*50*30	2
HFPG1-0.5	>500 V	<0.7 ns	1.5-2 ns decay	200kHz (4 MHz)	+50VDC	avr. output power ~1W	80*60*30	2
HFPG1P-0.5	-|-	-|-	-|-	4 MHz	-|-	avr.pow. >10W	100*60*60	4
HFPG1-2.5	>2.5 kV	<0.7 ns	1.5-2 ns decay	(2 MHz)	+100,+200VDC		120*80*60	4
HFPG1P-2.5	-|-	-|-	-|-	600kHz (2MHz)	-|-	avr.pow.>100W (liquid cooling)	240*220*200	4
HFPG2-1	>1000 V	<0.7 ns	<2 ns decay	(4 MHz)	+ 50 VDC	for high load (transm. anten.)	100*60*30	4
HFPG3-0.5	>500 V	<5 ns	10ns	(4MHz)	+ 50 VDC	efficiency >40%	80*60*30	2
HFPG3-0.05	>50 V	<0.7 ns	<2ns decay	25 MHz	+ 12 VDC		60*40*40	2
HFPG4-0.5	>500 V	<100ps	0.5 ns decay	(200kHz)	+50 VDC		100*60*30	4
HFPG4-2.5	>2.5 kV	<100ps	0.5 ns decay	(200kHz)	+15,+100 VDC		120*80*60	4
HFPG5-0.05	>50V	<100ps	0.5 ns decay	>20MHz	+12 VDC		80*40*40	2
HFPG6-25A	>25A	<1 ns	<2 ns decay	>1MHz	+24 VDC	for low load (laser pump)	200*60*30	2

CALL FOR PRICE & DELIVERY

PHONE: +7(812) 247-9996; FAX: +7(812) 247-5473; E-mail: alx@helen.ioffe.rssi.ru

ISBN 0-16-056562-6