28 February 1998
Source: http://www.house.gov/jec/hearings/02-25-8h.htm

Joint Economic Committee Hearing

Radio Frequency Weapons and Proliferation:

Potential Impact on the Economy

Wednesday, February 25, 1998

Witnesses:

James O'Bryon
Department of Defense

David Schriner
Electronic Warfare Association

Dr. Ira Merritt
Missile Defense Space Tech Center

Dr. Alan Kehs
U.S. Army Research Laboratories

Statement of Chairman Jim Saxton
Joint Economic Committee

Wednesday, February 25, 1998

Radio Frequency Weapons and Proliferation: Potential Impact on the Economy

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 *[below]* 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.

Dr. Alan Kehs is with U.S. Army Laboratories and will discuss the overall RF threat. Dr. Kehs has a BS and a MS in Electrical Engineering, and a MS and a PhD 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 coordinating committee.

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 BS 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.

Statement of

Mr. James F. O'Bryon

Deputy Director, Operational Test and Evaluation Live Fire Testing

Office of the Secretary of Defense

before the

Joint Economic Committee

United States Congress

Wednesday, 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 of

Mr. David Schriner

before the

Joint Economic Committee

United States Congress

Wednesday, February 25, 1998

"The Design and Fabrication of a Damage Inflicting RF Weapon by 'Back Yard' Methods"

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.

Statement of

Dr. Ira W. Merritt

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

before the

Joint Economic Committee

United States Congress

Wednesday, February 25, 1998

"Proliferation and Significance of Radio Frequency Weapons Technology"

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 weapons6 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 al12 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, Russia5. 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 target12. 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 long18.

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.

Statement of

Dr. R. Alan Kehs
Army Research Lab

before the

Joint Economic Committee

United States Congress

Wednesday, February 25, 1998

"The Radio Frequency Weapons Threat and Proliferation of Radio Frequency Weapons"

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 US 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 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.

Source: http://www.house.gov/jec/hearings/espionag/schweitz.htm

Statement by

Lieutenant General Robert L. Schweitzer
U.S. Army (Retired)

before the

Joint Economic Committee
United States Congress

June 17, 1997

Radio Frequency Weapons and the Infrastructure

I have been asked to talk to the overall subject of your hearing from a somewhat different perspective. Initially, it was to be from the one of what technology transfer means to a soldier. That part would have been fairly simple to address. Field soldiers are too busy to think much, if at all, about such transfers. That is, until they run across them on a battlefield where U.S. technology or materiel is being used against them. That happened in World War II when the residue of simpler technologies in the form of scrap metal was employed against us in the Pacific. It happened in Vietnam when some of our weaponry was obtained by our adversary. It happened again in Desert Storm when we ran across containers of U.S. materiel in the hands of Saddam Hussein's soldiers, materiel which had been channeled through Jordan. Then the fleeting reaction is one of anger and "why?" But soldiers--placed as they are since the time of the Roman legions in the sand, mud, rain and snow to fight decisive battles--are really too busy to brood much about such things. They are, however, grateful when Congress acts ahead of time to bar technology transfers, not only the simple ones of which I speak but the more serious, albeit subtle ones, which can affect the outcome of battles and wars.

Today there is a new class of radically new and important radio frequency weapons (RFW) which merits your attention as it emerges. And in this case, the horse is out of the barn. Transfers have occurred and are occurring. Equally true, however, is the fact that there are things that can be done to protect our nation, which is the underlying objective of today's hearing. Certainly one of these things is to recognize that export control documents, particularly the Militarily Critical Technologies List, needs to be reviewed to determine if radio frequency technologies should be considered in the same careful way we do nuclear technologies. I respectfully suggest that this is the case; stronger controls are needed. One example is Reltron tubes which went to a friendly nation, one who sells products widely--sometimes to nations who do not like us. These tubes, which can be small or large, generate intense radio frequency pulses and can be used as RF weapons.

Before we go further I wish to state clearly for you and for the public record that I do not speak for the Department of Defense, for any military service or any government agency. I come before you only as one who has researched this area for the past year and is writing a White Paper on the subject, one which will be offered to DoD for their use and disposition.

Some of you may know about radio frequency weapons, where they came from, what they can do and what the implications are.

Although there are a number of groups and individuals concerned with this subject, I have found that somewhat paradoxically the word has not really gotten out in Washington itself. Despite the existence of a Presidential commission, an Infrastructure Protection Task Force, a Critical Infrastructure Working Group, an Information Warfare School at the National Defense University, and other working groups, to include divisions on the Joint Staff in the Pentagon, as well as a few very dedicated and brilliant mid-level people in DoD, a general understanding is lacking. This is true not only of RFW, but of their immediate threat to our DoD and national infrastructure. Indeed the term "infrastructure" is so amorphous that it lacks impact if not meaning. One of our first tasks will be to define what is the military and economic infrastructure and what in it is susceptible and vulnerable to RF weapons.

Some 90 to 100 references in 26 pages of the 70-page Quadrennial Defense Review speak to this new threat, but only to a discerning reader; the name for the class is not used. On the other hand, a recent search of the Internet found 2,400 to 2,800 references, while yet another, more thorough search found many tens of thousands of documents where the key words "radio frequency weapons" appear. Some very good people have written books and articles on the subject, the first revealing article known to me appeared in 1987 in the Atlantic Monthly, but for many reasons the knowledge is diffused. In the public sector the subject has yet to draw any real attention or concerted action.

To help set the stage, recognize with experts like a former NSA Director that we are the most vulnerable nation on earth to electronic warfare. This thought is echoed by a former CIA Deputy Director, and a former Deputy Attorney General who forecast that we will have an electronic Pearl Harbor if we do not accept a wake up call. Our vulnerability arises from the fact that we are the most advanced nation electronically and the greatest user of electricity in the world.

On the military side, as in the civilian sector, our current superiority is based on microelectronics. To prevail against us, an adversary must cripple, destroy or deny access to those same microelectronics. Can an adversary do so? Very likely, as this hearing will bring out. All of our military doctrine assumes extensive use of sophisticated electronics and communication systems to ensure information dominance and overwhelming battlefield success. As is the case with our civilian infrastructure and economy, our current dependence is large and will continue to grow. Because our battlefield success and the well being of our civilian economy--with which this committee is especially charged–-are so dependent upon the effectiveness of our microelectronic-based systems, we should fully understand any technology that might be used to defeat our systems. This is particularly true of the newly emerging threat of radio frequency weapons. And even more importantly, we must develop countermeasures before such weapons are used against us.

Before going further, let me explain what these weapons are, where the Russian work has gone since 1949 and the applications of these weapons. If you are interested--as I believe you will be--you may wish to bring before you successive panels of our own leading scientists and experts. I have talked to many of them, heard them make presentations at conferences, and read their articles and books. I will be pleased to provide your staff with names of those who could provide this or other committees with a better understanding. I am also willing to assist in any way that might be helpful.

First of all, an RF weapon is one that uses intense pulses of RF energy to destroy ("burnout") or degrade ("upset") the electronics in a target. These weapons can be employed on a narrow beam over a long distance to a point target. They are also able to cover broad targets. They are categorized as high power microwave (HPM) weapons and ultra wide band (UWB) weapons.

The phrase non-nuclear electromagnetic pulse is sometimes used, because these weapons, which are indeed non-nuclear, project the same type of pulse we first learned of in conjunction with nuclear weapons. As a practical matter, a piece of electronic gear on the ground, in a vehicle, ship or plane does not really care whether it is hit by a nuclear magnetic pulse or a non-nuclear one. The effect is the same. It burns out the electronics. The same is true of the computers in this Senate office building, in industry, or on Wall Street.

There is another way these weapons can be delivered to a target, military or civilian. Here the term RF

munitions, or RFM is used. Yet these too are properly called RF weapons. These small munitions contain high explosives that produce radio frequency energy as their primary kill mechanism. In the hands of the skilled Russian scientists, these munitions come as hand grenades, mortar rounds, or large artillery shells or missiles. Generally, they produce a short but very intense pulse. While not yet fully understood and with some uncertainties argued as to their capabilities, many scientists are convinced the weapons actually exist. Without making any claims as to what they can do, I offer the following list from open source FSU literature of some nine smaller RF munitions or weapons:

- Magnetohydrodynamic Generator Frequency (MHDGF)
- Explosive Magnetic Generator of Frequency (EMGF)
- Implosive Magnetic Generator of Frequency (IMGF)
- Cylindrical Shock Wave Source (CSWS)
- Spherical Shock Wave Source (SSWS)
- Ferromagnetic Generator of Frequency (FMGF)
- Superconductive Former of Magnetic Field Shock Wave (SFMFSW)
- Piezoelectric Generator of Frequency (PEGF)
- Superconducting Ring Burst Generator (SCRBG)

Some of these weapons are said by the Russians to be now available as a hand grenade, a briefcase-like object, a mortar or artillery round.

Applications or potential targets (like those of the larger High Power Microwave weapons) would include all military computers, circuit boards, or chips, of any description, and include the following key components of our military and national infrastructure. They would have equal impact on civilian targets with the advantage less power would be required. Recall that the term "infrastructure" lacks clear meaning, but would include things like:

- The national telecommunications systems
- The national power grid
- The national transportation system, to include especially the FAA but also such simple things as our traffic lights (with consequent gridlock)
- The mass media
- Oil and gas control and refining
- Manufacturing processing, inventory control, shipment and tracking
- Public works
- Civil emergency service
- Finance and banking systems (to include bank's ability to dispense cash)

This list of potentially vulnerable targets could and should be extended to include airplanes, ships, vehicles and the like. Of interest is the fact that we are doubly vulnerable because we are, and will remain, in an era of dual use of military and civilian systems. For example, 90% of our military communications now passes over public networks. If an electromagnetic pulse takes out the telephone systems, we are in deep double trouble because our military and non-military nets are virtually inseparable. It is almost equally impossible to distinguish between the U.S. national telecommunications network and the global one. What this means is that it is finally becoming possible to do what Sun Tzu wrote about 2000 years ago: to conquer an enemy without fighting. The paradigm of war may well be changing. If you can take out the civilian economic infrastructure of a nation, then that nation in addition to not being able to function internally cannot deploy its military by air or sea, or supply them with any real effectiveness--if at all.

Since 1949, the intense interest of the former Soviet Union in developing these weapons appears to have resulted from their recognition that they could not match the capability of Western electronics, and their belief that RFW have the potential to be effective against our sophisticated electronics. It is far less clear to me and to others why they are willing to transfer and proliferate the RF technologies they have developed so carefully and so well, but that they are clearly doing so. Should you wish, a future hearing by this or another committee could go into more detail.

President Yeltsin proposed to President Clinton a joint program for a "plasmoid defense" against ICBM's.

While it is unclear to many scientists what President Yeltsin meant, such a defense, if attainable, might presumably set up a shield which would ionize the atmosphere and cause missiles to fail. Official Russian journals and publications show keen interest and provide many details about these weapons. A great amount of information is flowing continuously from three former Soviet Republics on their past and current programs.

We do know that the reduction in military spending by the FSU and many Western nations is prompting the defense industries of many countries to offer advanced weaponry to foreign customers to further their own research, development and industrial capabilities. This trend is almost certain to grow over the next 10 years.

From unclassified sources, we know that Russia, Ukraine, the United Kingdom, China, Australia and France are well ahead in this field, while Germany, Sweden, South Korea, Taiwan and Israel are emerging and have ample details of the Russian work and of the proceedings of more than 20 years of international conferences. Without going into any classified matters one may reasonably infer that the pariah nations have similar interests and some certainly have the financial resources to develop or procure RF weapons.

Russian and FSU information on RFW has been moving across borders for many years. International conferences beginning in 1949 have been a principal source of technology transfer. Scientists here and abroad have long exchanged papers, letters and, with increasing frequency, telephone calls.

- The first Megagaussing Conference on the generation of high power electromagnetic pulses took place in 1949 in Frascati, Italy. Russian scientists were key players in what has become a long series of presentations on the generation of electromagnetic power. Present at this and many subsequent conferences was the U.S. inventor of RF weapons, Dr. Max Fowler. His picture was placed over the center of the Moscow desk of one of his Russian counterparts who is a leader in the Russian development of the smaller version of these weapons. The latter is a key figure in the offer to sell RFW and RFM or their technologies to others.
- EUROEM Conferences have been meeting (with name changes) for perhaps some 20 years at about two-year intervals. At the 1994 conference which was held in Bordeaux, France, the Russians made public many details of their long work in these weapons. Some of their papers deal with the strategy, tactics and techniques for the use of offensive RF weapons. Among nations participating were Iran and Iraq. At this conference the Russians talked about selling their technology and weapons to prospective buyers. I am told that subsequently a large number of nations have engaged them in some form of negotiations. Some of these "buyers" raise legitimate concerns.
- The BEAMS conference (with name changes) has been meeting about every two years since 1975.
- The EUROEM Conference met in Albuquerque in 1996; the BEAMS Conference met that same year, I believe in Prague. Attendance was open to all nations.
- The next EUROEM and BEAMS conferences will meet in 1998 in the Middle East, two weeks apart in Tel Aviv and Haifa, respectively.
- An International Pulse Power Conference held their tenth conference under that name in 1995, but has existed under other names for a longer period of time.
- The International Particle Accelerator Conference has also met for more than 20 years.
- The American Physical Society has a Plasma Physics Division which hosted (for more than 20 years) many conferences. Usually each one has several sessions on microwave generation.
- And there are more. . .

Understanding the number, frequency and long standing nature of these conferences, you can perhaps better appreciate why I earlier said that the horse is out of the barn. Of interest, too, is the role of the United States in these conferences. Indisputably, the U.S. is the scientific powerhouse of the world. We have initiated and hosted a number of these conferences, funded many of them to a significant degree, and played a prominent role at all. While we gain some information, our scientists will readily acknowledge the net advantage is always to other attendees.

Put another way, from a narrow technology transfer standpoint we have thus far lost more than we gained. However, even prior to the Internet no one could control the flow of ideas, especially among scientists. They like to talk especially about what they have achieved, and how they solve theoretical and practical problems. For decades our scientists have found their Russian counterparts to be brilliant, dedicated and creative. Personal relations are important and some have developed, but they are exceptional. For the most part the Russians have

been ambiguous about their great work and often are mistrustful of Americans. We should move to change that by closer and warmer contacts as well as by efforts to enter into joint ventures--with all the travails that accompany such efforts. The Russians are intensely interested in our comments and some professional appreciation by their scientific peers of their decades of work on the offensive use of RF weapons. In my humble opinion they would prefer to work with our own distinguished scientists rather than others, but will sell their technology and products to others. I believe there is a real potential for joint ventures which could serve to constrain to some degree the proliferation of these weapons, especially to those who would do us harm.

To return to the earlier point about the need for better controls of technology transfer, consider these two counterpoints which illustrate the problem:

- First: Although RF weapon components are on the Critical Technologies List, there are no up to date DoD guidelines or directives on this subject. An attempt to do so was made two years ago when little was known about the subject. As a consequence, decisions within the U.S. scientific community are becoming harder and dicier to make. There is a lack of clear policy guidance and direction.
- Second: The first point is illustrated by the transfer of the Reltron microwave tubes. These tubes, which generate radio frequency power, cost a great deal of money to produce and test. The U.S. is the leader in high-power tubes and their associated power systems, but the market is really thin. Our tube industry has no current buyers here in the U.S. Without major contracts from foreign countries (France, the United Kingdom, Germany and Israel, among others), our tube industry will die. We will lose contact with real customers and become dependent on foreign hardware for our systems. Ultimately we will increase the difficulties that must be overcome to develop HPM applications for any future DoD use. Almost certainly we would know less--almost nothing--about what was going on in this area. For their part the Europeans and others would not cease to procure; they would simply undertake their own development. So our high power microwave scientific community told the State Department on balance to approve the transfer, which State did. Inevitably one consequence will be to advance the work of others and ultimately the production of RF devices to be used wherever and however by whomever. Note well, however: there is no guarantee that friendly countries will not sell the devices they produce to unfriendly, even hateful people.

It would also appear that there are other proliferation and transfer concerns of interest to this committee, simply because there is so much accurate how-to-do information in the open literature and on the Internet. Several countries have RFW programs and Russia says it has sold some technologies to these countries. At least one of these countries has acknowledged such a transfer. The crux of the difficulty in controlling these transfers is best illustrated by the fact that High Power Microwave weapons look like ordinary radars. With a dish or horn antenna, and a van with a power source, an RFW would look like a new, used or renovated radar. Used ones are offered for sale today in military surplus and commercial catalogs. Other catalogs offer for sale the components to put together lower power, but also very low cost items, that once assembled could be used effectively against the infrastructure.

Users of the new weapons can be criminals, individuals or organized gangs of narco or domestic terrorists--or a determined, organized, well-funded foreign adversary, either a group or nation who hates us.

The Russians, as noted, led with this work starting in 1949 with theory. By 1961, they were doing research, as documented in their numerous unclassified scientific articles. Experiments began in the seventies and proceeded to testing as described in their publications. Many of these weapons appeared in written descriptions, some photographs and diagrams in the nineties. Strategy, doctrine, tactics and techniques are all laid out in rather clear form. Please note all of this is unclassified information.

There is a legitimate question about the intelligence aspect of all of this. Our intelligence community largely proceeds on the operating principle followed in the Cold War: A threat is not validated until it is fielded. Well and good; hard evidence is essential.

But the question may fairly be asked: does that principle serve us well in the present day? Suppose we were to take a Russian or FSU-designed weapon, fabricate it in the U.S. and test it here. If the results were to meet the standards of performance and capabilities now claimed by the Russians, would we then have a validated threat? The answer to the capabilities may be forthcoming this month because at an unclassified level one of our

national labs is doing just that. Another lab has purchased cheap, off the shelf components and will test its lower power device this month. Their engineers and I believe it will indeed work against infrastructure and light military targets.

There is a great deal of other corroborating evidence which at least argues for the existence--which is still disputed in some quarters--of these weapons: one minor one is an International Institute for the Prevention of Offensive RF Weapons, located in Philadelphia. Why such an institute if there are no such things? Evidence as to the capabilities of the weapons may be found in such recent statements as China's declared intention to purchase three RF weapons derived from the Russian technology. Another is the series of reliably reported discussions within the IRA of their intention to seek RF weapons for use against the London financial system in lieu of bombs and explosives. Consider, too, the recent statement by Sweden they have used these devices in experiments to stop cars at 100 yards, as well as their reported claim that RF weapons have been used against their financial institutions. A similar but much disputed statement has been reported by the London Times concerning British financial and banking institutions. The Los Angeles Police Department had done some successful work with vehicles in the interests of public safety and to halt fleeing suspects. Advantages of the larger high power microwave RF weapons include:

- Low cost per engagement
- All weather
- Instantaneous engagement times
- Simplified pointing and tracking
- Possible to engage multiple targets
- Deep magazines–simplified logistics (can "fire" or pulse as long as there is power in the generator)
- Non-lethal to humans when properly adjusted
- Well suited to covert operations because of lack of signature; deniability
- Not able to detect attacks; silent when used without explosive devices

The RFM offer many of the same advantages, offset only by the sound of the explosion that detonates them and produces the rise in pulse energy.

Unless we choose to be, we are not without courses of action. Some of these could be explored at a future hearing. Some preliminary thoughts are offered today:

- We either fully understand nor control this technology.
- We have not begun to work on defenses , especially for our vulnerable infrastructure.
- We need to first scope the problem, determine susceptibilities and vulnerabilities, then test.
- All of this, to include any appropriate hardening of existing components, will take many years.
- There are other courses of corrective action, but all will take time to acquire and apply.
- The first step might well be to bring forward our real RF experts in DoD and the scientific community who know what needs to be done.

We need to go at this problem with a step-by-step sensible approach. No budget buster is proposed. Even if Congress had ready funds, a grandiose national solution is not the way to go.

We can start by scoping the problem and then by applying some of the same low-cost components that are now used in the ever expanding information technologies. Examples are surge-like protectors, plasma limiters, diodes, and metal covers. Parallel or redundant systems are another technique.

We are good at managing risks. We should no longer hesitate to reduce the impact of the threat, or to give our intelligence community the guidance to open up (some would say revise) their approach to this problem. Clearly the United States Congress will play a key role in whatever we do, or choose not to do, and our top leadership should focus on the longer term. But we should begin now in a sensible, modest way.

Three things we want to keep foremost in mind:

- Do not throw a lot of money at this problem. Funds don't exist; the best solutions will have to be devised.
- Do not tell DoD or the Services to take this out of their budgets. They are over stretched now and it would

be wrong to tell them to pay for protection of the civilian infrastructure.
- Do not continue to do what we have been doing and ignore the problem.
