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.

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 systems1, 2, 3. He further popularized these munitions with articles in Russian naval journals and in other professional journals and magazines4.

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 it5

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.