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.

JEC Return Home