Click here to view PowerPoint presentation; Press Esc to exit

Intentional Electromagnetic Interference – EM Terrorism

Dr. Robert L. Gardner
Consultant to Joint Program Office for Special Technology Countermeasures
Naval Surface Warfare Center
Electromagnetic & Solid State Technologies Division
17320 Dahlgren Road
Dahlgren, VA 22448-5100
USA

GardnerRL@nswc.navy.mil

No accompanying paper was provided –
Presentation speaking notes are provided below.

SLIDE ONE

The problem of electromagnetic terrorism is recognized world wide as a potential problem for critical electronic systems including aircraft, communications and control systems, and related parts of the infrastructure. This discussion will cover the potential sources of EM terrorism, the potential effects and what the community can and should do about it.

SLIDE TWO

This talk will attempt to define EM terrorism or its more polite name, Intentional Electromagnetic Interference.

We will then talk about the sources and the consequences of their actions. There has been significant public debate on an international scale on this issue about the problem and what the EMC community can do.

SLIDE THREE

IEMI is distinct from normal noise in that normal noise is a random environmental effect. IEMI is malevolent. That is, the attacking waveform can be chosen to most effectively damage the target system.

SLIDE FOUR

Damaging fields can be transmitted by a number of classes of people. They range from the guy who won't turn off his cell phone on a plane to the state sponsored weaponeer. The last class is not really of interest to this group.

SLIDE FIVE

These people are not mean but they are dangerous.

Gardner, R.L. (2002) Intentional Electromagnetic Interference – EM Terrorism. In *Tactical Implications of High Power Microwaves* (pp. 38-1 – 38-6). Meeting Proceedings RTO-MP-SCI-119, Paper 38 Notes. Neuilly-sur-Seine, France: RTO. Available from: http://www.rto.nato.int/abstracts.asp.

SLIDE SIX

The few examples we have of this actual activity are from criminals in Chesnya. Alarm systems defeated. Police radio nets jammed.

SLIDE SEVEN

These are the examples reported by Lovorov and confirmed by Fortov.

SLIDE EIGHT

The EM terrorist has more resources, although a fairly robust system can be assembled from surplus radars for a few 10s of thousands of dollars.

One important issue and that is of intent. IEMI can cause severe damage, even death, but the most likely outcome is electronics failure. A terrorist, therefore, may choose more convention means for direct terror. IEMI can be an enabler, however, as in the defeat of an alarm to system to rob a bank.

SLIDE NINE

This slide is just for completeness. There is very little the EMC community can do about these people.

SLIDE TEN

The effects of the easily available sources can be severe. A surplus radar could upset electronics at a fair distance.

SLIDE ELEVEN

To give you an idea how radio frequency sources work, here is a block diagram. The source generates the energy. The antenna directs it and the radio frequency fields propagate to the outside of the target. As noted, if you don't have test gear to support the direct illumination, you can inject currents and/or fields at the penetrations into the system.

SLIDE TWELVE

Some IEMI sources can be quite small. Of course, they must be applied quite close to the target electronics.

Truck mounted sources allow more flexibility in source parameters, but they are more difficult to get near the target without detection.

Direct injection eliminates the losses inherent in field propagation. Russian papers at EMC Zurich (Fortov) have discussed this topic.

SLIDE THIRTEEN

Almost any system that is run by electronics (almost everything) can be affected by IEMI. Consequences of some failures can be deadly or cause widespread damage, even death in the case of medical equipment.

SLIDE FOURTEEN

The US does not legally require compliance with EMI standards so poorly designed equipment that is susceptible widespread. Europe does have legal standards, but they are not everywhere.

SLIDE FIFTEEN

It is unfortunate that more serious attention isn't paid to EMI/EMC standards. It would make the EM Terrorist's job much more difficult.

SLIDE SIXTEEN

There has been a good of public discussion of EM Terrorism. These are some of the forums for that discussion.

SLIDE SEVENTEEN

There was well researched article in the New York Review of Books that attributed the crash of TWA 800 to electromagnetic energy. I do not accept the conclusion, but the article discussed the issues well.

Popular Science had a cover article on the "e-bomb". The article suggested that the damage caused by the e-bomb compared well with that of a nuclear weapon. That conclusion is nonsense, but is an example what is found in the press on this subject.

EMC magazine carried an article 15 years ago that predicted the use of truck mounted EM weapons to upset computers from a distance. The scenario was very much like that of some of the US testing elsewhere in this symposium.

The television program 20/20 carried a demonstration of some simple RF weapons and their use. They even upset the star's Corvette.

The Internet has numerous articles on various weapon concept. Some are fanciful. Others are relatively accurate.

SLIDE EIGHTEEN

The Joint Economic Committee held hearings on the threat of RF weapons. The different speakers approached the problem from different perspectives, but all concluded that RF weapons were a problem for the infrastructure. This testimony has been used to support Congressional interest funding in this area.

SLIDE NINETEEN

These are some of the arguments used to support the case to consider RF weapons in electronic design.

The first requirement is the existence of sources of sufficient power. There are enough sources on the open market and described elsewhere in this conference.

The effects those sources cause is less often discussed in public, although much information has been presented to you in this conference. Effects have been reported at very low levels.

The examples described earlier from Loborev and Fortov are the only real examples of EM Terrorism so far reported and supported.

SLIDE TWENTY

On a less public note: The JPO-STC has performed a demonstration of easily available RF sources. The work was described by Dr. Stoudt in this conference and at earlier meetings of SCI-019.

SLIDE TWENTY-ONE

Many of the electromagnetics and EMC conferences over the last four years have had some level of EM Terrorism discussion. Recently those discussions have blossomed into full invited and contributed sessions with 8 to 20 papers in each session. The International Conference on Electromagnetics in Advanced Applications held one of the best and it has a full paper Proceedings.

SLIDE TWENTY-TWO

The International Union of Radio Science is a large (3000 participants) organization that is part of the International Council of Scientific Unions which is, in turn, a part of UNESCO. Like the UN, members are countries, not individuals.

The 43 countries voted unanimously to support a resolution supporting the importance of research in EM Terrorism and protection of the civilian infrastructure from these criminal acts.

URSI Commission E formed an international working group on Intentional Electromagnetic Interference headed by Manuel Wik of Sweden.

SLIDE TWENTY-THREE

Since URSI is not a standards making nor regulative body it can only encourage certain types of research and provide a forum for that research. URSI has done both for EM Terrorism and is encouraging the appropriate groups to write standards.

SLIDE TWENTY-FOUR

This is the text of the URSI resolution on IEMI.

SLIDE TWENTY-FIVE

The International Electrotechnical Commission is in the process of creating standards for IEMI. There are two working groups involved chaired by Dave Giri and Fred Tesche.

SLIDE TWENTY-SIX

As member nations of NATO we have a responsibility to help protect our citizens from attack regardless of the technology or source of the threat. EM terrorism represents such a threat. We can protect ourselves best by educating the various NATO staffs on electromagnetics threats, and insisting that the critical infrastructure equipment that we purchase be properly protected from electromagnetic threats.

SLIDE TWENTY-SEVEN

Much of the equipment currently used by is NATO built of commercially available electronics. The public also depends on this same equipment for its infrastructure. The infrastructure (power, water, communications, medical equipment) is critical to the function of the military and the civilian economy. The public's awareness is primarily from movies and novels. As part of the military mission we should help educate the public and support the hardening of infrastructure equipment, regardless of end use.

SLIDE TWENTY-EIGHT

These are some of the questions we should continue to address. These questions are still current and are research topics that need solution.

SLIDE TWENTY-NINE

We have agreement though URSI and other forums that EM terrorism is problem. After that statement, however, there is little agreement. Certainly, we need to install the means of detecting EM terrorism so that we can attribute EM terrorism problems to the correct source or investigate other causes when appropriate. Education is desirable, but how and who funds it? Should there be enforceable standards? Is more research required?, by whom?, who funds? Some issues are sensitive from a security point of view. What level of protection should we afford the vulnerability levels of a personal computer? A civilian aircraft?