Brief Historical Review and Bibliography for Intentional Electromagnetic Interference (IEMI)

William A. Radasky*1 and Mats Bäckström2

1Metatech Corporation, 358 S. Fairview Ave., Suite E, Goleta, CA 93117 USA, wradasky@aol.com
2Saab Aeronautics, SAAB AB, SE-581 88 Linköping, mats.backstrom@saabgroup.com

Abstract

In the late 1990s, concerns were raised that the advancement of solid state high power electromagnetic sources and more advanced antennas systems could allow terrorists, criminals and hackers to interfere with the operation of modern electronic systems. In particular there was great concern that the critical infrastructures (e.g. power, telecommunications, transportation, etc.) could be disrupted using new technologies. Scientists and engineers throughout the world began to evaluate potential threats and their ability to create upset and damage; this field of study was initially known as EM Terrorism, but was changed to the more encompassing term of Intentional Electromagnetic Interference (IEMI). This paper reviews the early history of this field and provides a bibliography of important papers covering the overall threat, the development of potential weapons, the susceptibility of equipment and systems, protection methods and standardization.

1. Introduction

Although there were a few early papers dealing with the subject of intentional interference of electronics [1], there were three separate, significant events in 1999 that were responsible for informing the technical community of the importance of the topic. These including a workshop on EM Terrorism at the EMC Zurich Symposium in February 1999 [2], the decision by the International Electrotechnical Commission (IEC SC 77C) to add IEMI to its standardization program in June 1999 and the decision by URSI to publish a “Resolution of Criminal Activities using Electromagnetic Tools” in August 1999 [3]. The term IEMI was coined at EMC Zurich in 2001 [4] to replace the term, EM Terrorism”. Standards written by IEC SC 77C in later years also used the term IEMI [5]. In 2004 the IEEE EMC Society published a Special Transactions Issue on HPEM and IEMI that is a good reference for those who wish to understand the field [6].

In the past 15 years there have been literally hundred of papers written dealing with IEMI, and the purpose of this paper is to highlight some of the important papers covering the topics of the overall threat, the development of potential weapons, the susceptibility of equipment and systems, the development of protection methods and standardization in the field. Each of these topics is mentioned in separate sections with important references listed. Because of space limitations, we will not be able to list all important papers, but will try to reference those that are broad in their coverage.

2. The Overall Threat of IEMI

Some early papers are included here along with more recent publications. These papers discuss the possible scenarios that could used against commercial electronics along with a few cases where attacks were threatened or did occur.

3. The Development of Potential Weapons

The development of compact electromagnetic sources and antennas has been significant over the years especially in the area of broadband sources. The impulse radiating antenna (IRA) development allows the efficient launching of fast rising pulses. The IEC also has documented levels of source development dependent on the capabilities of those building them.


4. The Susceptibility of Equipment and Systems

Great progress has been made over the years testing different types of commercial equipment against both narrowband and wideband electromagnetic field transients and conducted transients (due to both coupled fields and to injected voltages) to determine susceptibility levels for equipment. It is difficult to pick the “best” sets of data, but an attempt is made by the authors here. In addition the method of classifying narrowband and wideband waveforms was an important development for dealing with the IEMI threat [5].


5. Protection Methods

Protection methods for IEMI include classical electromagnetic shielding, cable protection and also detection of an attack. Papers covering these topics are included below.

6. Standardization

Most of the standards published covering IEMI are from the IEC, however, the ITU-T, Cigré and the IEEE have also been active in the field. It should also be noted that many of the authors publishing in this field have been active in the standardization work of IEC SC 77C.


7. Conclusions

Significant progress has been made over the years in the field of IEMI to understand the threat, the susceptibility of equipment and systems, and to develop protection methods that can be standardized. The problem is a large one and will require future work to fully understand the most cost-effective ways to protect against this threat.

8. References