The threat of Intentional Electromagnetic Interference (IEMI) against modern critical infrastructures: Awareness and Protection

Stylianos C. Panagiotou
National Center for Scientific Research "Demokritos"
Institute of Informatics and Telecommunications
Integrated Systems Laboratory
Athens, Greece
email: stelios.panagiotou@iit.demokritos.gr

Stelios C. A. Thomopoulos
National Center for Scientific Research "Demokritos"
Institute of Informatics and Telecommunications
Integrated Systems Laboratory
Athens, Greece
email: scat@iit.demokritos.gr

Abstract— **The issue of intentional electromagnetic interference (IEMI) attacks against modern critical infrastructures is addressed. A description of how an IEMI attack is implemented and the categories of the relevant radio frequency weapons are provided and the effects of an IEMI incident on a targeted system are thoroughly examined. Moreover, techniques associated with electromagnetic interference mitigation and protection, as well as their advantages and disadvantages, are presented along with examples of how these techniques can be tailored to effectively address the particular consequences derived from IEMI events. Novel protection methods are proposed.**

Keywords- electromagnetic interference, radio frequency weapons; high power microwave; infrastructure protection; hardening measures; shielding; filtering; surge protective devices;

I. INTRODUCTION

IEMI, also known as Electromagnetic Terrorism, is the intentional, malicious generation of electromagnetic energy, introducing noise or signals into electric and electronic systems, thus disrupting, confusing or damaging these systems for terrorist or criminal purposes. IEMI can also be considered as a cyber attack since it corrupts data and damages critical data assets. Moreover, there is a worldwide trend to include IEMI to the broader category denoted as cyber threats.

A definition combining cyber and IEMI is following:

— **Cyber EMI attack** is any deliberate action involving the use of electromagnetic energy to control the domain characterized by the use of and the electromagnetic spectrum to store, modify, and/or exchange data via networked systems and associated physical infrastructures.

— **Cyber EMI protection** is the passive and/or active means taken to protect electronics and/or access to the electromagnetic spectrum from any effects of friendly or enemy employment of cyber EMI that degrades, neutralizes, or destroys ability to store, modify, and/or exchange data via networked systems and associated physical infrastructures.

Two factors determine in general the vulnerability of a target:

1. Coupling modes possible between the interfering source and the targeted equipment (front door or back door coupling)
2. The level of energy coupled that will damage or destroy a particular target.

The effects of IEMI on a system are taken into account in this work, including (in order of decreasing severity):

- permanent physical damage,
- permanent function failure,
- temporary upset (with operator intervention),
- performance reduction,
- temporary upset (without operator intervention).

II. PROTECTION MEASURES AGAINST IEMI

Protection methods against IEMI have been surveyed in this work, including:

- Organizational practices (e.g. physical keep-out perimeters),
- Use of T-R limiters in radar and antenna systems,
- Controlling the directivity pattern of an antenna so that nulls are created along the directions of the interfering incoming signals (e.g. exploitation of smart antennas),
- Use of frequency selective surfaces on the radome to limit the out of band energy reaching the antenna,
- Electromagnetic Shielding,
- Earthing and Grounding topologies
- Use of circuit protection technologies (limiting with surge protective devices and filtering),

Furthermore novel hardening architectures are introduced.

This work is supported by the "HIPOW" EU research project ("Protection of Critical Infrastructures against High Power Microwave Threats" HIPOW-FP7-SEC-2011-284802).