Threat of Electromagnetic Terrorism

Leassons learned from documented IEMI Attacks

Frank Sabath
Division 300: Balanced Nuclear Protection Measures and Nuclear Hardening, Electro-Magnetic Effects, Fire Protection
Bundeswehr Research Institute for Protective Technologies and NBC Protection (WIS)
Munster, Germany
FrankSabath@bundeswehr.org

Abstract— **The existing threat by criminal (intentional) use of electromagnetic tools is discussed. Reported Intentional Electromagnetic Interference (IEMI) attacks and similar incidents will be analyzed and discussed in regard to aspects like motivation and technical skills of the culprits, characteristics of the generated IEMI environment as well as effects on the target systems. Concluding common characteristics will lead to a discussion of the technological challenge of recognition and identification of an IEMI attack as well as backtracking of observed malfunction and destructions to an external IEMI environment.**

Keywords- IEMI, HPEM, documented attacks, threat analysis

I. INTRODUCTION

This paper discusses to what extent the technological development in the last decades resulted in an ascent of the threat by criminal use of high power electromagnetic systems. It starts with an overview about Intentional Electromagnetic Interference (IEMI) attacks and similar incidents which were reported in freely accessible literature. The paper continues by analyzing these observed attacks and IEMI caused effects concerning motivation and technical skills of the culprits, characteristics of the generated IEMI environment and effects on the target systems. Finally, the section "lessons learned" will conclude common characteristics and discuss aspects of recognition and identification of an IEMI attack as well as backtracking of observed malfunction and destructions to an external IEMI environment.

II. DOCUMENTED CRIMINAL USAGE OF ELECTROMAGNETIC TOOLS

Public literature [1,2,5] has reported eight criminal usages of electromagnetic tools:

1. In Japan, criminals used an EM disruptor to interfere with the computer of a gaming machine and falsely triggered a win.
2. In St. Petersburg, a criminal used an EM disruptor to disable a security system of a jeweler store.
3. In Kizlyar, Dagestan, Russia, Chechen rebel command disabled police radio communication using RF jammers during a raid.
4. In multiple European cities (e.g. Berlin) criminals used GSM-Jammers to disable the security system of limousines.
5. In Russia, Chechen rebels used an EM disruptor to defeat a security system and gain access to a controlled area.
6. In the Netherlands an individual disrupted a local bank IT network because he was refused loan.
7. In Moscow, the normal work of one automatic telephone exchange station has been stopped as a result of remote injection of a voltage in to a telephone line.

There have also been several documented incidents caused by EM devices that could be employed by criminals or terrorists [2, 5]. The IEMI cases presented above clearly point out that today the threat by (criminal) IEMI attacks on electronic systems already exists.

III. LESSONS LEARNED

The documented cases of criminal IEMI attack will be analyzed with regard to (1) motivation and needed skills of the offender, (2) risk aspects of the IEMI environment and (3) the caused effect on the target system (including consequences). The reported attack will be analyzed to deduce common characteristics that will enable an assessment of the current threat by IEMI terrorism and develop appropriate countermeasures.

REFERENCES

[1] V. Fortov, Yu. Parfenov, L. Siniy and L. Zdoukhov, "Russian Research of intentional electromagnetic disturbances over the past ten years", Proceedings of the AMEREM 2006, Albuquerque (NM, USA), July 2006.

[2] R. Hoad and I. Sutherland, "The forensic utility on detecting disruptive electromagnetic interference", Proceedings of the 6th European Conference on Information Warfare and Security (ECIW 2007), July 2007.

[3] D.V. Giri, "Documented Electromagnetic Effects (EME)", Proceedings of the EUROEM 2008, Lausanne, Switzerland, July 2008.

[4] F. Sabath and H. Garbe, "Risk Potential of Radiated HPEM Environments", Proceedings of the 2009 IEEE International Symposium on Electromagnetic Compatibility, Austin (TX), USA, August 2009, pp. 226-231

[5] Sabath, F.; , "What can be learned from documented Intentional Electromagnetic Interference (IEMI) attacks?," General Assembly and Scientific Symposium, 2011 XXXth URSI , vol., no., pp.1-4, 13-20 Aug. 2011