What can be learned from documented Intentional Electromagnetic Interference (IEMI) Attacks?

Frank Sabath

Federal Ministry of Defense, Armament Directorate IV 6, Fontainengraben 150, 53123 Bonn, Germany,
Frank.Sabath@ieee.org

Abstract

The existing threat by criminal (intentional) use of electromagnetic tools is investigated. 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.

1. Introduction

In 1999 at its XXVIth General Assembly in Toronto the URSI adopted a resolution on Criminal Activities using Electromagnetic tools [1]. This resolution was intended to make the public aware of the increasing danger by possible criminal use of electromagnetic systems and the potentially serious nature of effects caused by criminal activities using electromagnetic tools on electronic systems, in particular if they are parts of critical infrastructure. The resolution highlighted the fact that criminal activities using electromagnetic tools can be undertaken covertly and the used electromagnetic sources might hardly be identified. As physical boundaries such as fences and walls can be penetrated by electromagnetic fields, these barriers show no effective protection. The final goal of the resolution was to encourage additional research to understand potential interference mechanisms, collect data on the susceptibility of electronic systems and to develop appropriate protection measures.

During the decade since the resolution on Criminal Activities using Electromagnetic tools was adopted several research programs around the world have investigated physical mechanism of electromagnetic interferences and caused effects on electronic equipment and systems. At the same time, the development of components for high-power electromagnetic (HPEM) sources has achieved notable progress. As a result, high-power systems difficult or impossible to build ten years ago are now being used for an increasingly wide variety of applications and are available on the free market.

This paper discusses to what extent the technological development 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.

2. Documented criminal Usage of Electromagnetic Tools

In 1999 URSI Commission E defined criminal activities using electromagnetic tools as an 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. In order to underline the intentional character the electromagnetic compatibility community coined for these kinds of actions the term Intentional Electromagnetic Interference (IEMI).

Public literature [2, 3, 4] 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.

978-1-4244-6051-9/11/$26.00 ©2011 IEEE

2. In St. Petersburg, a criminal used an EM disruptor to disable a security system of a jeweler store. The reports mentioned that building the EM disruptor posed a technological challenge similar to assemble a home microwave oven.
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 London, UK, a city bank was the target of a blackmail attempt whereby the use of EM disruptors was threatened to be used against the banks IT-system.
7. In the Netherlands an individual disrupted a local bank IT network because he was refused loan. He constructed a briefcase-size EM disruptor, which he learned how to build from the internet. Bank officials did not realize that they had been attacked or what had caused the disruption until the assailant was caught.
8. 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. As a result two hundred thousand people had no phone connection for one day.

There have also been several documented incidents caused by EM devices that could be employed by criminals or terrorists [2, 5]. On the target side results of susceptibility investigations as well as reports on observed electromagnetic effects show that IEMI attacks might result in serious consequences or catastrophic situations. However, the IEMI cases presented above clearly point out that today the threat by (criminal) IEMI attacks on electronic systems already exists.

3. Analysis of documented IEMI Attacks

In the context of IEMI threats it is important to understand the types of crime which could be perpetrated using EM tools, the technology of employed IEMI environments and the provoked effects so that specific countermeasure and protection concepts can developed and established. In this section 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).

3.1 Offender

The motivation and technical skills which characterize the offender in the presented cases of criminal IEMI attacks are displayed in Table 1. In five cases the crime was committed for money and in four of these cases the EM tools were used to arrange the actual criminal action by suppression of service. The fact that the culprits committed the crime for money could be used in a counter attack strategy, as the culprits have to collect the money. In contrast, the motivation for the last two cases was to damage electronic systems. As electromagnetic fields can penetrate physical barriers, offender might undertake the crime covertly. In fact, in both cases the reason for the observed effect has been unknown for some period of time. If we focus on the technical skills needed to operate the IEMI source we learn that in all cases the challenge was very low (e.g. amateur to technician). Practically, we can assume that everyone who wants to use EM tools for criminal purpose will be able to do so.

3.2 IEMI Environment

In [7] Sabath and Garbe presented a methodology for the assessment of the risk potential of a given IEMI environment. The methodology employs the aspects threat level, mobility and technological challenge to determine the likelihood of occurrence of a given IEMI environment and compiles them into a risk potential. Unfortunately, the reports about IEMI attacks focus more on the caused effects than on details of the used IEMI sources. Therefore, we get hardly sufficient information to determine the threat level but the provided information enables us to estimate the technological challenge posed by the design and assembly of the IEMI source and its mobility. The aspect mobility summarizes the capability of an IEMI source to come close to the target system. Table 2 shows the characterizing

Table 1: Motivation and technical skills of offender.

	Case	Motivation	Skills/ Knowledge
1	Gaming machine	Robbery	1: Amateur/ Internet
2	Jeweler store	Robbery	1.5: Amateur – Technician
3	Police radio communication	Suppression/ Denial of service	2: Technician
4	Car security system	Robbery	1 : Amateur/ Internet
5	Russian security system	Suppression / Denial of service & Robbery	2: Technician
6	UK Bank	Blackmail/ Robbery	1.5: Amateur – Technician
7	NL Bank	Payback/ Criminal damage	1 : Amateur/ Internet
8	Telephone Moscow	Criminal damage	unknown

parameters of IEMI sources that are used in reported IEMI attacks. As expected, most IEMI sources are categorized by higher degrees of mobility, which means that they are able to operate undiscovered in urban environment (*very mobile*) or within a building or transportation system, e.g. train or airplane, (*highly mobile*).

3.3 Effects on IEMI Target Systems

A systematic classification of effects caused by IEMI environments is discussed in [6]. The most suitable method for the analysis of observed IEMI attacks is the classification by its criticality, as it provides the essential information on the function, isolated from its duration or physical mechanism. The criticality scales from *No effects* over *Interference* and *Degradation* to *Loss of main function*. Depending on the nature of the system under attack, implications of the observed effects might not be limited to the system. An interference or degradation of a critical (electronic) system could result in an economic loss or a catastrophic situation. Therefore, the consequence of an IEMI attack is of vital interest and must be considered in an overall threat analysis. For the purpose of this paper the consequence of observed IEMI attacks are rated *technical defect*, *economical loss*, *economical damage* and *disaster*.

The effects of the reported IEMI attacks, their criticality and consequences are listed in Table 3. Due to the motivation of the culprits, in cases 2 to 5 the caused effects are suppression of the main function with a criticality rated by *degradation* or (temporary) *loss of main function*. In the cases of the suppressed police radio communication as well as the Russian security system the consequences are unknown. In case 2 and 4 the IEMI attacks resulted in some economic loss, as intended by criminals. The case of IEMI attack on the computer system of the NL bank resulted in more serious consequences. In addition to repair costs and loss of data, the loss of confidence in the reliability of the bank resulted in a long term economic damage. The situation was worsened by the fact that the IEMI attack has been undetected for a certain period of time.

Table 2: Technology, technological challenge and mobility of used IEMI sources.

	Case	Technology	Technological Challenge	Mobility
1	Gaming machine	RF Gun (EM Disruptor)	1: Low tech system	4: Very mobile
2	Jeweler store	EM Disruptor	2: Medium tech system	3.5: (Very) mobile
3	Police radio communication	Jammer	2: Medium tech system	3.5: (Very) mobile
4	Car security system	GSM Jammer	1: Low tech system	5: Highly mobile
5	Russian security system	unknown	2: Medium tech system	5: Highly mobile
6	UK Bank	unknown		
7	NL Bank	HPM-Source	1: Low tech system	4: Very mobile
8	Telephone Moscow	Direct Injection	No information available	No information available

Table 3: Effect, criticality and consequence of observed IEMI attacks.

	Case	Effect	Criticality	Consequence
1	Gaming machine	malfunction	interference	Unjustified win/ economic loss
2	Jeweler store	suppression of main function	degradation/ loss of main function	economic loss
3	Police radio communication	suppression of main function	degradation	unknown
4	Car security system	suppression of main function	loss of main function	economic loss
5	Russian security system	suppression of main function	degradation	unknown
6	UK Bank	unknown	unknown	economic loss
7	NL Bank	malfunction/ destruction of components	degradation/ loss of main function	defect → lack of confidence & economic damage
8	Telephone Moscow	Shut-down	loss of main function	economic damage

4. Lessons Learned

The IEMI cases presented clearly point out that today the threat by (criminal) IEMI attacks on electronic systems already exists. IEMI sources and their components are available on the free market and the knowledge needed for the assembly as well as the operation can be gained from open literature and the internet. Available IEMI sources are small and highly mobile, e.g. they are able to come close to the target systems. Those systems generate an EM environment that is capable to cause at least a malfunction or (temporary) set up of electronic components. The caused effects might be used to prepare the actual criminal activity.

As electromagnetic fields propagate through material without any alteration of the material IEMI attacks barely leave useful and provable traces. In addition, the complexity of systems often hinders error analysis and received error pattern point to internal causes. Build in test systems are optimized to identify internal errors and malfunctions. As a consequence unpredicted conditions will be mapped to predicted (internal) errors. A user of a system which is subjected to IEMI environment is unlikely to have any sensation or perception of the (external) electromagnetic stress. With the lack of an indication of the threat and in combination with misleading error patterns the user is perhaps more likely to blame faulty hardware or software errors, rather than an ongoing IEMI attack. Consequently, any IEMI counterattack measure depends on a monitoring of the (external) electromagnetic fields that enables an independent indication of high electromagnetic stress that belongs to IEMI attacks.

5. References

1. URSI, "URSI resolution on criminal activities using electromagnetic tools", URSI resolutions adopted at the Toronto general assembly, Minutes of the XXVIth General Assembly of the URSI, 1999.
2. United States Department of Homeland Security, "The Threat of radio frequency weapons to critical infrastructure facilities", *TSWG and DTEO Publication,* August 2003.
3. 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.
4. 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.
5. D.V. Giri, "Documented Electromagnetic Effects (EME)", Proceedings of the EUROEM 2008, Lausanne, Switzerland, July 2008.
6. F. Sabath, "Classification of electromagnetic effects at system level", *Ultra-Wideband, Short-Pulse Electromagnetics 9*, pp. 325 – 334, 2010.
7. 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