Detection of Disruptive Intentional Electromagnetic Interference (IEMI) to Information Systems and Processes

Richard Hoad[(1)]
(1) QinetiQ, EMC Group, Cody Technology Park, Farnborough, Hants, GU14 0LX, UK, +44 (0) 1252 393604, rhoad@qinetiq.com

Disruptive and denial of service attacks to Information Technology (IT) equipment, systems, or processes are extremely undesirable, especially if these systems are used for national infrastructure, physical security, financial, or safety critical applications.

Intentional Electromagnetic (EM) disruption is a specialised threat to Information security. This attack form exploits the fact that electrical and electronic systems (which comprise the basis of modern information infrastructures) are affected by and therefore susceptible to Radio Frequency (RF) energy. However, the ability of Intentional EM Interference sources to generate significant disruption to the availability of information systems and supporting electronics is speculative and therefore the risk posed is extremely difficult to quantify. Given these constraints it is difficult to cost effectively recommend the installation of specific hardening measures for risk mitigation, since the risk is poorly understood or quantified, even though very effective countermeasures for IEMI and EM denial of service attacks exist.

Detection of IEMI is likely to be a useful step towards identification of the need for balanced and proportionate hardening of information infrastructures. Means of detecting IEMI do not readily appear in the open literature, and therefore do not appear to be widely developed. Development of EM detectors similar in many ways to conventional software based Intrusion Detection Systems (IDS) may assist current information security professionals to understand the risk to information security posed by the relatively new area of EM disruption.

This paper discusses the manifestation of EM disruption, explores the requirements for an EM detection system, and provides details of some deployed concepts.