ID 063

A Comparison of Intentional EMI, Cyber and Physical Threats and Protection

R. Hoad, C. Harper, B. Petit and A. Fernandes

QinetiQ Ltd.
Farnborough, Hampshire, UK
rhoad@qinetiq.com

***Abstract*— Recently QinetiQ has been commissioned to undertake several surveys of Critical National Infrastructure (CNI) sites in the UK and the US to evaluate the risk to the sites from Intentional Electromagnetic Interference (IEMI). This paper summarizes some observations from these surveys and our interactions with CNI owners/operators. This paper also compares and contrasts the IEMI threat with Cyber (computer network attacks) and physical threats.**

Keywords- IEMI, Electromagnetic Compatibility, Critical National Infrastructure, Cyber

I. Introduction

Intentional Electromagnetic Interference (IEMI) is of growing concern to Critical National Infrastructure (CNI) asset owners/operators, largely because of the recent expansion in the use of embedded electronic systems for control and diagnostic purposes and the growing availability of capable IEMI sources [1]. New legislative drivers such as the SHIELD ACT in the USA [2] and the perceived risk from Cyber threats are forcing CNI asset owners and operators to consider their vulnerability to these relatively new threats.

A definition of Cyberspace is “an operational domain whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interconnected information-communication technology (ICT) based systems and their associated infrastructures” [3]. However, mostly the term Cyber is associated with a rather narrow definition of the threat which can be summarized as Computer Network Attack (CNA), whereby both the source of the threat and the target are ICT based. Examples of CNA include; hacking, malicious software (malware), Denial of Service (DoS) and Distributed Dos (DDoS), Botnets, and network intrusion [4].

Physical threats to the CNI are perhaps more familiar and can include, for example; bombing, arson, and theft.

II. Observations

A summary of observations of the difference in threat perception and protection are given in Table 1. These observations are ‘first hand’ and were identified from various Technical Visual Assessments (TVAs) of established functional CNI Sites in the UK and the US and of plans and designs for new sites yet to be built. The TVAs were conducted by QinetiQ in the last 24 months.

This paper explores these differences in a higher level of detail, providing examples where they have been observed.

TABLE I. A Summary of Observations

Cyber/Physical Threats	**IEMI Threats**
Most Infrastructure providers/operators have an individual(s) responsible for Cyber Security or ‘digital risk’ and Physical Security	Very few infrastructure providers presently acknowledge or recognize the IEMI threat – therefore they do not generally appoint someone to be responsible for IEMI protection
Cyber and Physical threats can affect confidentiality, integrity and availability	IEMI is primarily a threat to the availability of information/capable of denying service
Cyber exploits can be conducted from another continent, outside of one Nation’s legal jurisdiction. Physical threats require physical interaction with the asset	The range of IEMI threat sources can easily exceed the physical perimeter of a CNI asset but do not have the reach of Cyber threats
Cyber is fundamentally a risk to interconnected ICT networks. Physical threats are a risk to physical, tangible assets	IEMI can affect all unprotected electronic devices – not just interconnected ICT networks and can even affect electronic systems used to support physical security
Laws already exist for Cyber-crimes and Cyber Terrorism. Physical acts on a CNI site are covered by standard legal doctrine	Whilst it is illegal to transmit Radio Frequency signals without a license in many countries the act of procuring and using an IEMI source has not been legally tested
The manifestation of a Cyber disturbance can be subtle or severe but it is possible to recover an evidence trail. Physical threats tend to leave physical evidence	IEMI disturbances can leave very little or no physical evidence.
Cyber/Physical Protection	**IEMI Protection**
A wide variety of standards and guides are available to infrastructure designers to improve the physical and Cyber security of new facilities	Whilst design rules and standards exist to protect a new-build facility from IEMI, they are rarely mandated.
Cyber and Physical attack is often detectable – detectors are available and deployed	Whilst IEMI detection concepts are starting to become available, their adoption is uncommon
For Cyber threats, software patches can be used to rapidly mitigate vulnerabilities. Physical threats can be difficult to mitigate rapidly	IEMI threats can be difficult to mitigate rapidly
For Cyber threats Isolation and precise control of network connectivity boundaries (including the human behavioral boundary) massively reduces risk. Physical protection generally employs physical boundary controls	IEMI protection can make use of the physical protection boundary if it is constructed in a way that mitigates IEMI. For example perimeter fences that have good attenuation properties or provide adequate stand-off.

References

[1] EU FP7 Security Research Topic SEC-2011.2.2-2 Protection of Critical Infrastructure (structures, platforms and networks) against Electromagnetic (High Power Microwave (HPM)) Attacks http://cordis.europa.eu/search/index.cfm?, 2011

[2] HR 2417, US Congress, ‘“Secure High-voltage Infrastructure for Electricity from Lethal Damage Act ”or the “SHIELD Act ”, June 18 2013

[3] Kuehl D. (2008), ‘From Cyberspace to Cyberpower: Defining the Problem’, Information Resources Management College/National Defense University, Air Force Symposium 2008: Cyberspace, July 15 – 17 2008, Air University (AU) Maxwell AFB, USA.

[4] Singer P and Friedman A., ‘Cybersecurity and Cyberwar: What Everyone Needs to Know’, 6 February 2014