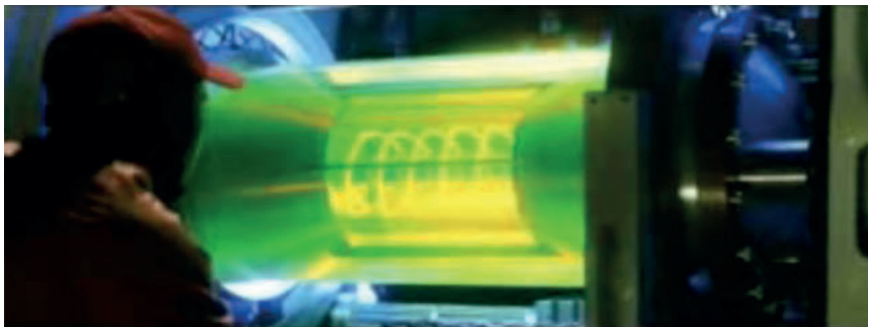
The emerging threat of tactical electromagnetic interference & its spread into non-defence sectors

by Paul Currie, Director, MPE Ltd

During the past five years intentional electromagnetic interference (IEMI) has emerged as a credible and increasingly likely threat to commercial and defence facilities alike, with a potentially crippling cost to individual organisations of such a localised attack.

Hollywood has long used electromagnetic interference (EMI) and electromagnetic pulse (EMP) phenomena as the de facto basis for sensational blockbuster movies. As far back as 1952, the classic science fiction film "The Day the Earth Stood Still" featured the widespread effects of such an EMP event, with cars stopping, lights going out and radios being silenced. More recently, "Ocean's Eleven" saw Don Cheadle's character activate an EMP generator, inadvertently blacking out most of Las Vegas.



EMP generator in 'Ocean's Eleven'

Similarly, since the 1990's, the electronics community has been discussing and reporting on the potential large-scale effects from such EMI and EMP events. Papers and presentations on the effects of a pulse generated by a high-altitude, nuclear type detonation (HEMP), or from natural phenomena such as geomagnetically induced currents (GICs) from solar storms, have become almost commonplace. The Lloyd's Report entitled "The Solar Storm Risk to the North American Electric Grid" published in 2013 is just one example. The impacts of such EMP events have also been widely acknowledged, with several guidelines and standards being published, such as the U.S. Department of Homeland Security's Electromagnetic Pulse (EMP) Protection and Restoration Guidelines for Equipment and Facilities, published in 2016.

Following the first Gulf War, several national strategies were developed, promulgating methods for initiating a "black-out" war by completely turning off the adversary's power via cyber, kinetic or EMP activity. Subsequently state sponsors of terrorism and terrorist networks such as ISIS have openly stated that they are exploring these same strategies as a means of delivering their threat. However, such activity is at a national or strategic level and, whilst the results of such large-scale EMP effects are generally recognised, the probability of such events taking place is considered to be relatively low.

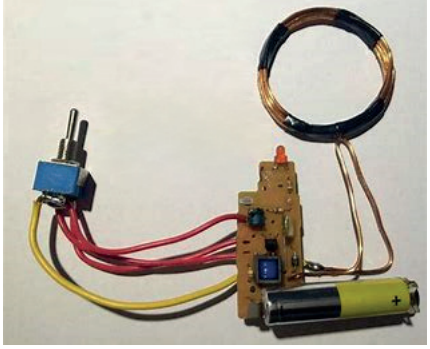
In more recent times, the discussion has progressed to concentrate on more directed, localised or tactical EMP events and has expanded beyond the defence arena to include commercial and industrial organisations, public authorities and their infrastructures.

It is understood that the effects of tactical EMP attacks are likely to be lesser than strategic EMP ones, but it is equally clear that the threat and probability of those attacks taking place are far greater. What is also recognised is that the likelihood of such EMP occurrences being intentionally generated has also significantly increased. This is commonly referred to as Intentional Electromagnetic Interference (IEMI).

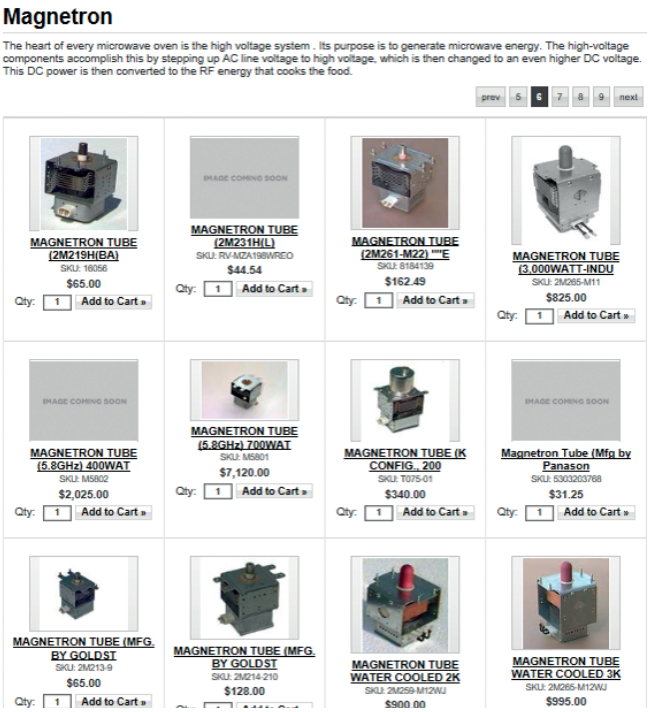
Such IEMI attacks may be driven by a political motive or financial gain, but could just as easily be motivated by a desire for peer group recognition or simply by the challenge of breaching complex computer systems.

That could be considered similar to computer hacking or high-level cyber-crime. Nevertheless, whilst the execution of cyber-crime activities calls for specialist skills and expensive and sophisticated equipment, IEMI can be unleashed with a minimum of technical knowledge and has a low cost-of-entry. What is more, the originators of cyber-crime are often eventually traced back and prosecuted. By contrast, unless a perpetrator can be caught in the brief act of delivering an IEMI attack, it is completely untraceable and leaves no evidential trail.

Any search of the Internet will yield a number of YouTube-type instructional videos, showing how to construct an IEMI device. Following such instructions requires little or no prior electrical knowledge, few tools and some common raw materials and components. You can then source your shopping list of these parts, generally available on the Internet, for no more than a few dollars, euros or pounds.



Portable DIY EMP device



Magnetron components on the Internet

The method of delivery of any such IEMI attack may differ and can range from a primitive homemade contrivance, a suitcase-type apparatus, up to vehicle-mounted, transportable devices. The method used may be determined by how much the perpetrator is prepared to spend. In carrying out any such IEMI or localised EMP threat, two factors are of primary importance. These are the amount of power that can be generated by the chosen device and how close it is to its target. In general terms, the more power that can be generated by a device and the nearer it is to the target, the greater the effects will be.

Suitcase-size EMP generator

Vehicle-mounted EMP generator

In cases where these two factors are diminished, the resulting effects may be limited to errors in data or outages with minor disruption to services or operations, or control room monitors freezing for a short period. But, given sufficient power and a reasonable proximity to the target, effects could easily result in entire systems going down and requiring the reset and reboot of servers. In the worst case scenario, the outcome would be the destruction of electronic equipment, where no data is recoverable from that system.

The most widespread, costly and potentially devastating are likely to be the repercussions of IEMI jamming computer systems inside the critical assets which run our communications, navigation

and broadcasting systems, public utilities, transportation, hospitals, datacentres, banks, financial institutions and commodity and stock exchanges. In this context there is a wealth of publicly available information relating to the U.S. power grid network and other vulnerable sectors of their national economy.

According to the U.S. Department of Energy's Lawrence Berkeley National Laboratory, the annual cost of short interruptions (lasting five minutes or less) to the American economy had risen from $52 billion in 2002 to $60 billion in 2014. Estimates from other publicly available information are that up to 25% of power disruptions have an undefined cause. It is now widely understood and accepted that a percentage of these undefined causes are the result of unintentional or intentional EMI or EMP activity.

Disturbingly, at an organisational level, S&C Electric's (S&C) 2018 State of Commercial & Industrial Power Reliability report found that 18% of companies surveyed had experienced a loss of more than $100,000 as a result of their worst outage, whilst half of customers surveyed had endured outages lasting more than one hour during the past year. The same survey revealed that 25% of companies reported experiencing at least one outage per month. Again, the view is widely held that a percentage of such system downtime is as a result of EMI or EMP activity.

Calculations show that, on average, organisations lose between $84,000 and $108,000 for every hour of IT system downtime, and a 2016 study by the Ponemon Institute for IT and data protection based in Michigan estimated that the cost of a datacentre outage in the USA had grown to $8,851 per minute.

A single hour of system downtime can cost up to $108,000

Until 2010 consideration of protection against such EMI and EMP events was almost exclusively limited to military installations and defence-focused organisations around the world. In the main this was due to the only available testing compliance Standards being the very onerous U.S. Mil-Std-188-125 and the UK's Def Stan 59-188. The cost to implement protection compliant with these Standards could be prohibitive.

More recently, the publication, for example, of the previously referenced Lloyds Report of 2013 along with the new IEC Standards for IEMI immunity test methods for equipment and systems (IEC 61000-4-36) and Radiated & Conducted HEMP protection (IEC 61000-4-23 & 24) published in 2015 has led to an increase in non-defence-related organisations considering, investing in and implementing protection against IEMI.

For instance, one of Scandinavia's largest power grid company owners has been implementing EMP protection for a number of years to add resilience to its network. In the USA, a major communications provider nationwide is now exploring in detail how they may best implement protection of their facilities, to ensure the continuity of the services they provide in the case of any localised EMI or EMP event.

This spread of EMI and EMP protection into commercial, public and utility sectors is only set to increase further, with a raft of new legislation and standards updates *either already introduced during 2018 or in consultation for introduction in the very near future.

The Network and Information Security (NIS) EU Law was published in May 2018. This EU Law requires any company providing essential services – such as in banking and finance, public sector, IT, healthcare and transport – to report henceforth all cyber security incidents caused by EMI, EMP or other threats and the extent of any resultant damage and disruption.

In the USA Mil-Std-188-125 is due to be updated, whilst in the UK Def Stan 59-188 is also rumoured to be being updated. Moreover the IEC is due to release further guidance regarding HEMP and IEMI (IEC 61000-5-10) during 2019. The Critical Infrastructure Protection Act (CIPA) in the USA has been with Congress since 2016 and is expected to be passed into legislation by 2020. This Act will make public utility organisations responsible for protecting their own systems and services against the effects of EMI and EMP events, or risk significant punitive fines, should those systems and services be affected as a direct result.

This shifting of responsibility to both private and public sector service providers for maintaining and protecting their services in the face of any tactical IEMI attack is a significant development. In addition to the potentially crippling physical, financial and reputational damage that they may cause, the repercussions of IEMI strikes could now be punishable in law, and consequently protective solutions to combat the threat have never been in greater demand.

Independent British defence electronics manufacturer MPE Ltd of Liverpool supplies resilient filter solutions for just this purpose to markets around the world. MPE has the experience of having provided over ten million filters for EMC, EMP and TEMPEST applications over the past 30 years and is the world's leading supplier of high-altitude electromagnetic pulse (HEMP) filters.

www.mpe.co.uk

Paul Currie

Founded in 1925, MPE Ltd of Liverpool designs and manufactures electromagnetic compatibility (EMC), electromagnetic pulse (EMP) and TEMPEST filters for use in defence and commercial applications. Paul Currie is a Director and co-owner of MPE Ltd. He is a Chartered Director (CDir) and Fellow of the Institute of Sales Management (ISM) and Institute of Directors (IoD). Paul has worked in the electronics industry for over 20 years and is a regular speaker on EMP and IEMI phenomena and protection at conferences and seminars around the world.

For further details of MPE's products and applications, please contact Paul Currie, Sales & Marketing Director, MPE Ltd, Hammond Road, Knowsley Industrial Park, Liverpool, L33 7UL, U.K. Tel +44 (0)151 632 9111. Cell +44 (0)7850 200 705.
Email pcurrie@mpe.co.uk. Website www.mpe.co.uk