The Electromagnetic Bomb - a Weapon of Electrical Mass Destruction

Carlo Kopp
Defence Analyst
Melbourne, Australia
Carlo.Kopp@aus.net
http://www.cs.monash.edu.au/~carlo/

ABSTRACT

High Power Electromagnetic Pulse generation techniques and High Power Microwave technology have matured to the point where practical E-bombs (Electromagnetic bombs) are becoming technically feasible, with new applications in both Strategic and Tactical Information Warfare. The development of conventional E-bomb devices allows their use in non-nuclear confrontations. This paper discusses aspects of the technology base, weapon delivery techniques and proposes a doctrinal foundation for the use of such devices in warhead and bomb applications.

1. Introduction

The prosecution of a successful Information Warfare (IW) campaign against an industrialised or post industrial opponent will require a suitable set of tools. As demonstrated in the Desert Storm air campaign, air power has proven to be a most effective means of inhibiting the functions of an opponent's vital information processing infrastructure. This is because air power allows concurrent or parallel engagement of a large number of targets over geographically significant areas [SZAFRANSKI95].

While Desert Storm demonstrated that the application of air power was the most practical means of crushing an opponent's information processing and transmission nodes, the need to physically destroy these with guided munitions absorbed a substantial proportion of available air assets in the early phase of the air campaign. Indeed, the aircraft capable of delivery laser guided bombs were largely occupied with this very target set during the first nights of the air battle.

The efficient execution of an IW campaign against a modern industrial or post-industrial opponent will require the use of specialised tools designed to destroy information systems. Electromagnetic bombs built for this purpose can provide, where delivered by suitable means, a very effective tool for this purpose.

2.The EMP Effect

The ElectroMagnetic Pulse (EMP) effect [1] was first observed during the early testing of high altitude airburst nuclear weapons [GLASSTONE64]. The effect is characterised by the production of a very short (hundreds of nanoseconds) but intense electromagnetic pulse, which propagates away from its source with ever diminishing intensity, governed by the theory of electromagnetism. The ElectroMagnetic Pulse is in effect an electromagnetic shock wave.

This pulse of energy produces a powerful electromagnetic field, particularly within the vicinity of the weapon burst. The field can be sufficiently strong to produce short lived transient voltages of thousands of Volts (ie kiloVolts) on exposed electrical conductors, such as wires, or conductive tracks on printed circuit boards, where exposed.

It is this aspect of the EMP effect which is of military significance, as it can result in irreversible damage to a wide range of electrical and electronic equipment, particularly computers and radio or radar receivers. Subject to the electromagnetic hardness of the electronics, a measure of the equipment's resilience to this effect, and the intensity of the field produced by the weapon, the equipment can be irreversibly damaged or in effect electrically destroyed. The damage inflicted is not unlike that experienced through exposure to close proximity lightning strikes, and may require complete replacement of the equipment, or at least substantial portions thereof.

Commercial computer equipment is particularly vulnerable to EMP effects, as it is largely built up of high density Metal Oxide Semiconductor (MOS) devices, which are very sensitive to exposure to high voltage transients. What is significant about MOS devices is that very little energy is required to permanently wound or destroy them, any voltage in typically in excess of tens of

Volts can produce an effect termed gate breakdown which effectively destroys the device. Even if the pulse is not powerful enough to produce thermal damage, the power supply in the equipment will readily supply enough energy to complete the destructive process. Wounded devices may still function, but their reliability will be seriously impaired. Shielding electronics by equipment chassis provides only limited protection, as any cables running in and out of the equipment will behave very much like antennae, in effect guiding the high voltage transients into the equipment.

Computers used in data processing systems, communications systems, displays, industrial control applications, including road and rail signalling, and those embedded in military equipment, such as signal processors, electronic flight controls and digital engine control systems, are all potentially vulnerable to the EMP effect.

Other electronic devices and electrical equipment may also be destroyed by the EMP effect. Telecommunications equipment can be highly vulnerable, due to the presence of lengthy copper cables between devices. Receivers of all varieties are particularly sensitive to EMP, as the highly sensitive miniature high frequency transistors and diodes in such equipment are easily destroyed by exposure to high voltage electrical transients. Therefore radar and electronic warfare equipment, satellite, microwave, UHF, VHF, HF and low band communications equipment and television equipment are all potentially vulnerable to the EMP effect.

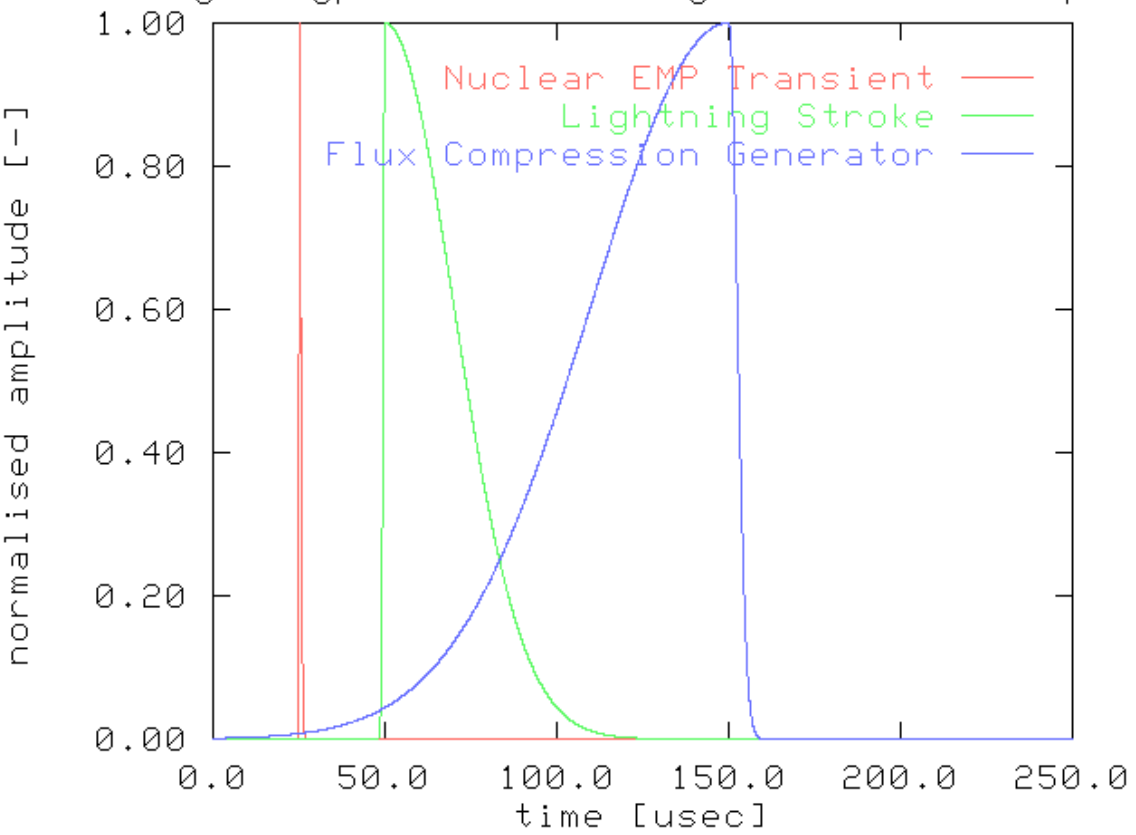
It is significant that modern military platforms are densely packed with electronic equipment, and unless these platforms are well hardened, an EMP device can substantially reduce their function or render them unusable.

3. The Technology Base for Conventional Electromagnetic Bombs

The technology base which may be applied to the design of electromagnetic bombs is both diverse, and in many areas quite mature. Key technologies which are extant in the area are explosively pumped Flux Compression Generators (FCG), explosive or propellant driven Magneto-Hydrodynamic (MHD) generators and a range of HPM devices, the foremost of which is the Virtual Cathode Oscillator or Vircator. A wide range of experimental designs have been tested in these technology areas, and a considerable volume of work has been published in unclassified literature.

This paper will review the basic principles and attributes of these technologies, in relation to bomb and warhead applications. It is stressed that this treatment is not exhaustive, and is only intended to illustrate how the technology base can be adapted to an operationally deployable capability.

Fig.1 Typical Electromagnetic Pulse Shapes



3.1. Explosively Pumped Flux Compression Generators

The explosively pumped FCG is the most mature technology applicable to bomb designs. The FCG was first demonstrated by

Clarence Fowler at Los Alamos National Laboratories (LANL) in the late fifties [FOWLER60]. Since that time a wide range of FCG configurations has been built and tested, both in the US and the USSR, and more recently CIS.

The FCG is a device capable of producing electrical energies of tens of MegaJoules in tens to hundreds of microseconds of time, in a relatively compact package. With peak power levels of the order of TeraWatts to tens of TeraWatts, FCGs may be used directly, or as one shot pulse power supplies for microwave tubes. To place this in perspective, the current produced by a large FCG is between ten to a thousand times greater than that produced by a typical lightning stroke [WHITE78].

The central idea behind the construction of FCGs is that of using a fast explosive to rapidly compress a magnetic field, transferring much energy from the explosive into the magnetic field.

The initial magnetic field in the FCG prior to explosive initiation is produced by a start current. The start current is supplied by an external source, such a a high voltage capacitor bank (Marx bank), a smaller FCG or an MHD device. In principle, any device capable of producing a pulse of electrical current of the order of tens of kiloAmperes to MegaAmperes will be suitable.

A number of geometrical configurations for FCGs have been published (for examples see REINOVSKY85, CAIRD85, FOWLER89) The most commonly used arrangement is that of the coaxial FCG. The coaxial arrangement is of particular interest in this context, as its essentially cylindrical form factor lends itself to packaging into munitions.

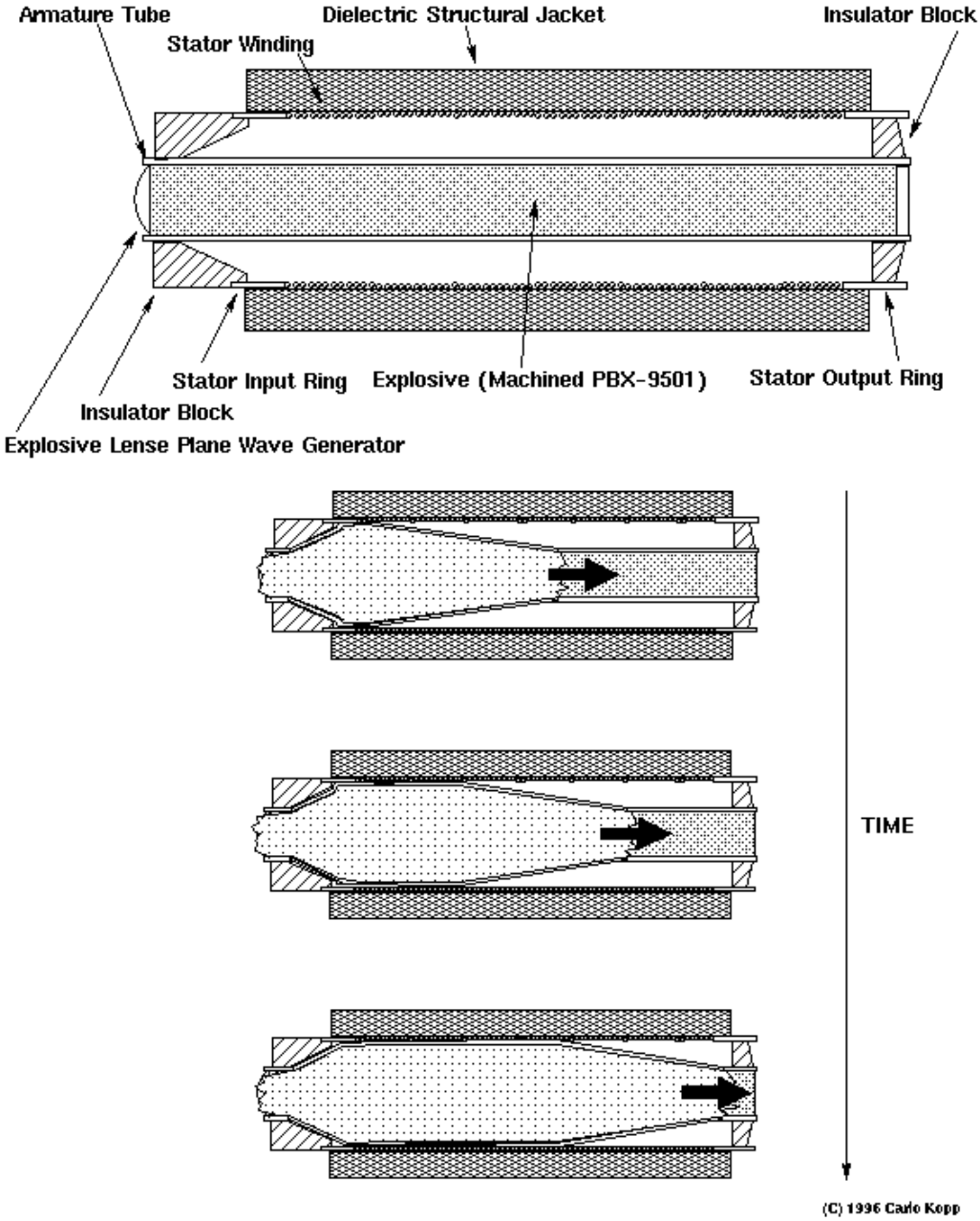


FIG.2 EXPLOSIVELY PUMPED COAXIAL FLUX COMPRESSION GENERATOR

In a typical coaxial FCG , a cylindrical copper tube forms the armature. This tube is filled with a fast high energy explosive. A number of explosive types have been used, ranging from B and C-type compositions to machined blocks of PBX-9501. The armature is surrounded by a helical coil of heavy wire, typically copper, which forms the FCG stator. The stator winding is in some designs split into segments, with wires bifurcating at the boundaries of the segments, to optimise the electromagnetic inductance of the armature coil.

The intense magnetic forces produced during the operation of the FCG could potentially cause the device to disintegrate prematurely if not dealt with. This is typically accomplished by the addition of a structural jacket of a non-magnetic material. Materials such as concrete or Fibreglass in an Epoxy matrix have been used. In principle, any material with suitable electrical and mechanical properties could be used. In applications where weight is an issue, such as air delivered bombs or missile warheads, a glass or Kevlar Epoxy composite would be a viable candidate.

It is typical that the explosive is initiated when the start current peaks. This is usually accomplished with a explosive lense plane wave generator which produces a uniform plane wave burn (or detonation) front in the explosive. Once initiated, the front propagates through the explosive in the armature, distorting it into a conical shape (typically 12 to 14 degrees of arc). Where the

armature has expanded to the full diameter of the stator, it forms a short circuit between the ends of the stator coil, shorting and thus isolating the start current source and trapping the current within the device. The propagating short has the effect of compressing the magnetic field, whilst reducing the inductance of the stator winding. The result is that such generators will producing a ramping current pulse, which peaks before the final disintegration of the device. Published results suggest ramp times of tens to hundreds of microseconds, specific to the characteristics of the device, for peak currents of tens of MegaAmperes and peak energies of tens of MegaJoules.

The current multiplication (ie ratio of output current to start current) achieved varies with designs, but numbers as high as 60 have been demonstrated. In a munition application, where space and weight are at a premium, the smallest possible start current source is desirable. These applications can exploit cascading of FCGs, where a small FCG is used to prime a larger FCG with a start current. Experiments conducted by LANL and AFWL have demonstrated the viability of this technique [KIRTLAND94, REINOVSKY85].

The principal technical issues in adapting the FCG to weapons applications lie in packaging, the supply of start current, and matching the device to the intended load. Interfacing to a load is simplified by the coaxial geometry of coaxial and conical FCG designs. Significantly, this geometry is convenient for weapons applications, where FCGs may be stacked axially with devices such a microwave Vircators. The demands of a load such as a Vircator, in terms of waveform shape and timing, can be satisfied by inserting pulse shaping networks, transformers and explosive high current switches.

3.2. Explosive and Propellant Driven MHD Generators

The design of explosive and propellant driven Magneto-Hydrodynamic generators is a much less mature art that that of FCG design. Technical issues such as the size and weight of magnetic field generating devices required for the operation of MHD generators suggest that MHD devices will play a minor role in the near term. In the context of this paper, their potential lies in areas such as start current generation for FCG devices.

The fundamental principle behind the design of MHD devices is that a conductor moving through a magnetic field will produce an electrical current transverse to the direction of the field and the conductor motion. In an explosive or propellant driven MHD device, the conductor is a plasma of ionised explosive or propellant gas, which travels through the magnetic field. Current is collected by electrodes which are in contact with the plasma jet [FANTHOME89].

The electrical properties of the plasma are optimised by seeding the explosive or propellant with with suitable additives, which ionise during the burn [FANTHOME89, FLANAGAN81]. Published experiments suggest that a typical arrangement uses a solid propellant gas generator, often using conventional ammunition propellant as a base. Cartridges of such propellant can be loaded much like artillery rounds, for multiple shot operation.

3.3. High Power Microwave Sources - The Vircator

Whilst FCGs are potent technology base for the generation of large electrical power pulses, the output of the FCG is by its basic physics constrained to the frequency band below 1 MHz. Many target sets will be difficult to attack even with very high power levels at such frequencies, moreover focussing the energy output from such a device will be problematic. A HPM device overcomes both of the problems, as its output power may be tightly focussed and it has a much better ability to couple energy into many target types.

A wide range of HPM devices exist. Relativistic Klystrons, Magnetrons, Slow Wave Devices, Reflex triodes, Spark Gap Devices and Vircators are all examples of the available technology base [GRANATSTEIN87, HOEBERLING92]. From the perspective of a bomb or warhead designer, the device of choice will be at this time the Vircator, or in the nearer term a Spark Gap source. The Vircator is of interest because it is a one shot device capable of producing a very powerful single pulse of radiation, yet it is mechanically simple, small and robust, and can operate over a relatively broad band of microwave frequencies.

The physics of the Vircator tube are substantially more complex than those of the preceding devices. The fundamental idea behind the Vircator is that of accelerating a high current electron beam against a mesh (or foil) anode. Many electrons will pass through the anode, forming a bubble of space charge behind the anode. Under the proper conditions, this space charge region will oscillate at microwave frequencies. If the space charge region is placed into a resonant cavity which is appropriately tuned, very high peak powers may be achieved. Conventional microwave engineering techniques may then be used to extract microwave power from the resonant cavity. Because the frequency of oscillation is dependent upon the electron beam parameters, Vircators may be tuned or chirped in frequency, where the microwave cavity will support appropriate modes. Power levels achieved in Vircator experiments range from 170 kiloWatts to 40 GigaWatts over frequencies spanning the decimetric and centimetric bands [THODE87].

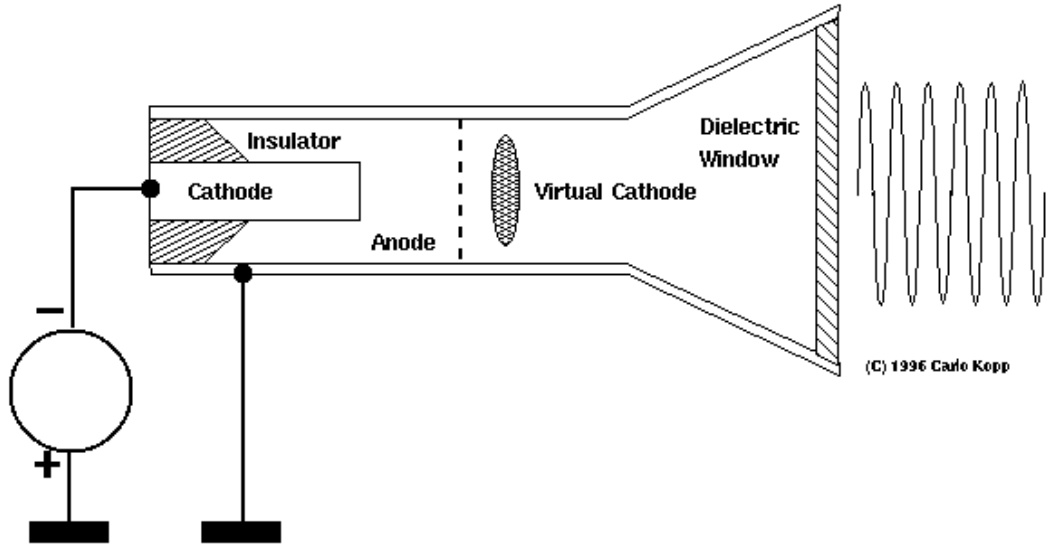


FIG.3 AXIAL VIRTUAL CATHODE OSCILLATOR

The two most commonly described configurations for the Vircator are the Axial Vircator (AV) (Fig.3), and the Transverse Vircator (TV). The Axial Vircator is the simplest by design, and has generally produced the best power output in experiments. It is typically built into a cylindrical waveguide structure. Power is most often extracted by transitioning the waveguide into a conical horn structure, which functions as an antenna. AVs typically oscillate in Transverse Magnetic (TM) modes. The Transverse Vircator injects cathode current from the side of the cavity and will typically oscillate in a Transverse Electric (TE) mode.

Technical issues in Vircator design are output pulse duration, which is typically of the order of a microsecond and is limited by anode melting, stability of oscillation frequency, often compromised by cavity mode hopping, conversion efficiency and total power output. Coupling power efficiently from the Vircator cavity in modes suitable for a chosen antenna type may also be an issue, given the high power levels involved and thus the potential for electrical breakdown in insulators.

4. The Lethality of Electromagnetic Warheads

The issue of electromagnetic weapon lethality is complex. Unlike the technology base for weapon construction, which has been widely published in the open literature, lethality related issues have been published much less frequently.

While the calculation of electromagnetic field strengths achievable at a given radius for a given device design is a straightforward task, determining a kill probability for a given class of target under such conditions is not.

This is for good reasons. The first is that target types are very diverse in their electromagnetic hardness, or ability to resist damage. Equipment which has been intentionally shielded and hardened against electromagnetic attack will withstand orders of magnitude greater field strengths than standard commercially rated equipment. Moreover, various manufacturer's implementations of like types of equipment may vary significantly in hardness due the idiosyncrasies of specific electrical designs, cabling schemes and chassis/shielding designs used.

The second major problem area in determining lethality is that of coupling efficiency, which is a measure of how much power is transferred from the field produced by the weapon into the target. Only power coupled into the target can cause useful damage.

4.1. Coupling Modes

In assessing how power is coupled into targets, two principal coupling modes are recognised in the literature:

- Front Door Coupling occurs typically when power from a electromagnetic weapon is coupled into an antenna associated with radar or communications equipment. The antenna subsystem is designed to couple power in and out of the equipment, and thus provides an efficient path for the power flow from the electromagnetic weapon to enter the equipment and cause damage.
- Back Door Coupling occurs when the electromagnetic field from a weapon produces large transient currents (termed spikes, when produced by a low frequency weapon) or electrical standing waves (when produced by a HPM weapon) on fixed electrical wiring and cables interconnecting equipment, or providing connections to mains power or the telephone network [TAYLOR92, WHITE78]. Equipment connected to exposed cables or wiring will experience either high voltage transient spikes or standing waves which can damage power supplies and communications interfaces if these are not hardened. Moreover, should the transient penetrate into the equipment, damage can be done to other devices inside.

A low frequency weapon will couple well into a typical wiring infrastructure, as most telephone lines, networking cables and power lines follow streets, building risers and corridors. In most instances any particular cable run will comprise multiple linear segments joined at approximately right angles. Whatever the relative orientation of the weapons field, more than one linear segment of the cable run is likely to be oriented such that a good coupling efficiency can be achieved.

It is worth noting at this point the safe operating envelopes of some typical types of semiconductor devices. Manufacturer's guaranteed breakdown voltage ratings for Silicon high frequency bipolar transistors, widely used in communications equipment, typically vary between 15 V and 65 V. Gallium Arsenide Field Effect Transistors are usually rated at about 10V. High density Dynamic Random Access Memories (DRAM), an essential part of any computer, are usually rated to 7 V against earth. Generic CMOS logic is rated between 7 V and 15 V, and microprocessors running off 3.3 V or 5 V power supplies are usually rated very closely to that voltage. Whilst many modern devices are equipped with additional protection circuits at each pin, to sink electrostatic discharges, sustained or repeated application of a high voltage will often defeat these [MOTO3, MICRON92, NATSEMI86].

Communications interfaces and power supplies must typically meet electrical safety requirements imposed by regulators. Such interfaces are usually protected by isolation transformers with ratings from hundreds of Volts to about 2 to 3 kV [NPI93].

It is clearly evident that once the defence provided by a transformer, cable pulse arrestor or shielding is breached, voltages even as low as 50 V can inflict substantial damage upon computer and communications equipment. The author has seen a number of equipment items (computers, consumer electronics) exposed to low frequency high voltage spikes (near lightning strikes, electrical power transients), and in every instance the damage was extensive, often requiring replacement of most semiconductors in the equipment [2].

HPM weapons operating in the centimetric and millimetric bands however offer an additional coupling mechanism to Back Door Coupling. This is the ability to directly couple into equipment through ventilation holes, gaps between panels and poorly shielded interfaces. Under these conditions, any aperture into the equipment behaves much like a slot in a microwave cavity, allowing microwave radiation to directly excite or enter the cavity. The microwave radiation will form a spatial standing wave pattern within the equipment. Components situated within the anti-nodes within the standing wave pattern will be exposed to potentially high electromagnetic fields.

Because microwave weapons can couple more readily than low frequency weapons, and can in many instances bypass protection devices designed to stop low frequency coupling, microwave weapons have the potential to be significantly more lethal than low frequency weapons.

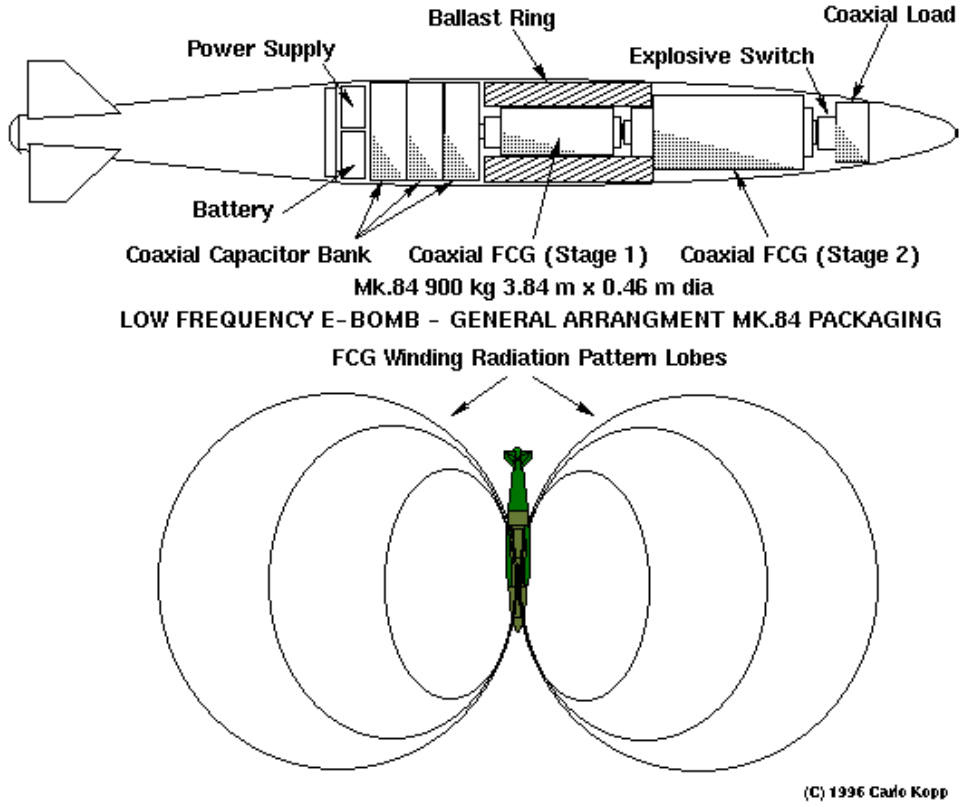


FIG.4 LOW FREQUENCY E-BOMB WARHEAD (MK.84 FORM FACTOR)

What research has been done in this area illustrates the difficulty in producing workable models for predicting equipment vulnerability. It does however provide a solid basis for shielding strategies and hardening of equipment.

The diversity of likely target types and the unknown geometrical layout and electrical characteristics of the wiring and cabling infrastructure surrounding a target makes the exact prediction of lethality impossible.

A general approach for dealing with wiring and cabling related back door coupling is to determine a known lethal voltage level, and then use this to find the required field strength to generate this voltage. Once the field strength is known, the lethal radius for a given weapon configuration can be calculated.

A trivial example is that of a 10 GW 5 GHz HPM device illuminating a footprint of 400 to 500 metres diameter, from a distance of several hundred metres. This will result in field strengths of several kiloVolts per metre within the device footprint, in turn capable of producing voltages of hundreds of volts to kiloVolts on exposed wires or cables [KRAUS88, TAYLOR92]. This suggests lethal radii of the order of hundreds of metres, subject to weapon performance and target set electrical hardness.

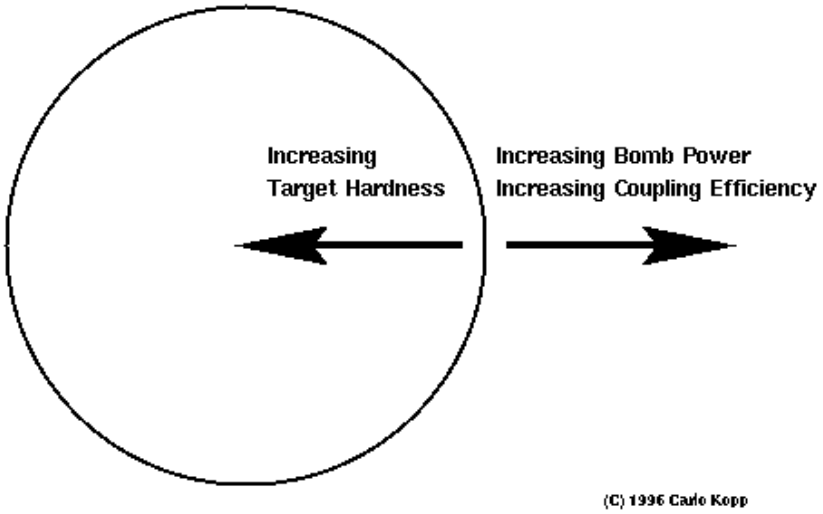


FIG.5.1 E-BOMB LETHAL RADIUS

4.2. Maximising Electromagnetic Bomb Lethality

To maximise the lethality of an electromagnetic bomb it is necessary to maximise the power coupled into the target set.

The first step in maximising bomb lethality is is to maximise the peak power and duration of the radiation of the weapon. For a given bomb size, this is accomplished by using the most powerful flux compression generator (and Vircator in a HPM bomb) which will fit the weapon size, and by maximising the efficiency of internal power transfers in the weapon. Energy which is not emitted is energy wasted at the expense of lethality.

The second step is to maximise the coupling efficiency into the target set. A good strategy for dealing with a complex and diverse target set is to exploit every coupling opportunity available within the bandwidth of the weapon.

A low frequency bomb built around an FCG will require a large antenna to provide good coupling of power from the weapon into the surrounding environment. Whilst weapons built this way are inherently wide band, as most of the power produced lies in the frequency band below 1 MHz compact antennas are not an option. One possible scheme is for a bomb approaching its programmed firing altitude to deploy five linear antenna elements. These are produced by firing off cable spools which unwind several hundred metres of cable. Four radial antenna elements form a "virtual" earth plane around the bomb, while an axial antenna element is used to radiate the power from the FCG. The choice of element lengths would need to be carefully matched to the frequency characteristics of the weapon, to produce the desired field strength. A high power coupling pulse transformer is used to match the low impedance FCG output to the much higher impedance of the antenna, and ensure that the current pulse does not vapourise the cable prematurely.

Other alternatives are possible. One is to simply guide the bomb very close to the target, and rely upon the near field produced by the FCG winding, which is in effect a loop antenna of very small diameter relative to the wavelength. Whilst coupling efficiency is inherently poor, the use of a guided bomb would allow the warhead to be positioned accurately within metres of a target. An area worth further investigation in this context is the use of low frequency bombs to damage or destroy magnetic tape libraries, as the near fields in the vicinity of a flux generator are of the order of magnitude of the coercivity of most modern magnetic materials.

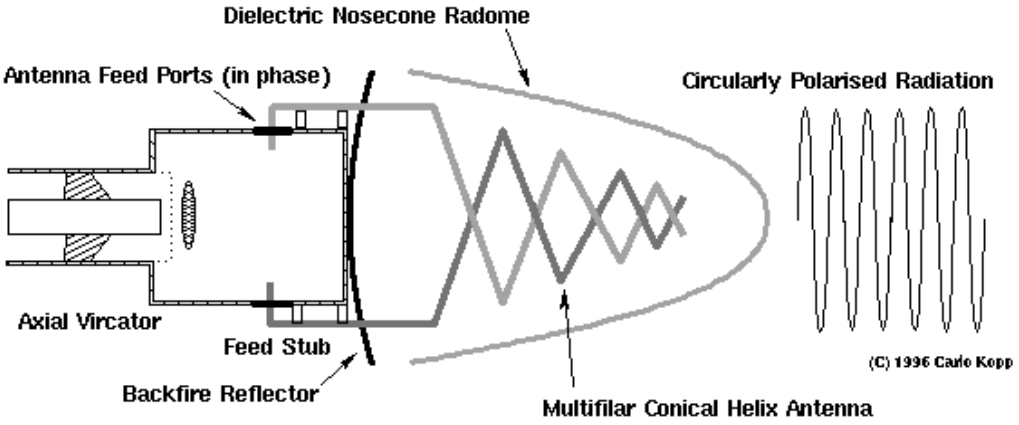
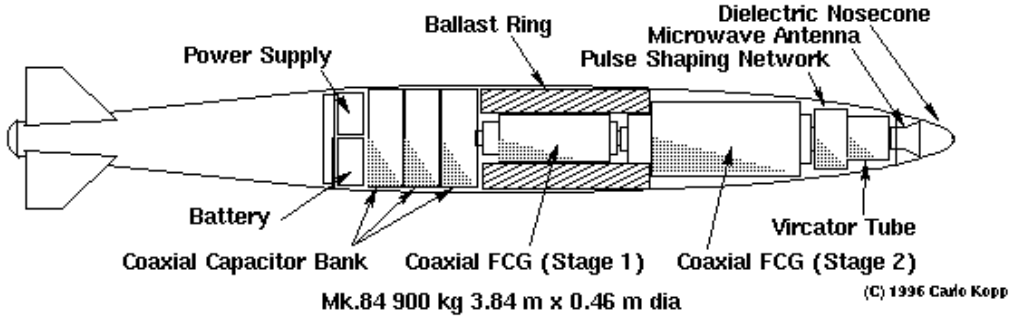


FIG.5.2 EXAMPLE OF VIRCATOR/ANTENNA ASSEMBLY

Microwave bombs have a broader range of coupling modes and given the small wavelength in comparison with bomb dimensions, can be readily focussed against targets with a compact antenna assembly. Assuming that the antenna provides the required weapon footprint, there are at least two mechanisms which can be employed to further maximise lethality.



HIGH POWER MICROWAVE E-BOMB - GENERAL ARRANGMENT MK.84 PACKAGING
WARHEAD USING VIRCATOR AND 2 STAGE FLUX COMPRESSION GENERATOR

FIG.6 HPM E-BOMB WARHEAD (Mk.84 FORM FACTOR)

The first is sweeping the frequency or chirping the Vircator. This can improve coupling efficiency in comparison with a single frequency weapon, by enabling the radiation to couple into apertures and resonances over a range of frequencies. In this fashion, a larger number of coupling opportunities are exploited.

The second mechanism which can be exploited to improve coupling is the polarisation of the weapon's emission. If we assume that the orientations of possible coupling apertures and resonances in the target set are random in relation to the weapon's antenna orientation, a linearly polarised emission will only exploit half of the opportunities available. A circularly polarised emission will exploit all coupling opportunities.

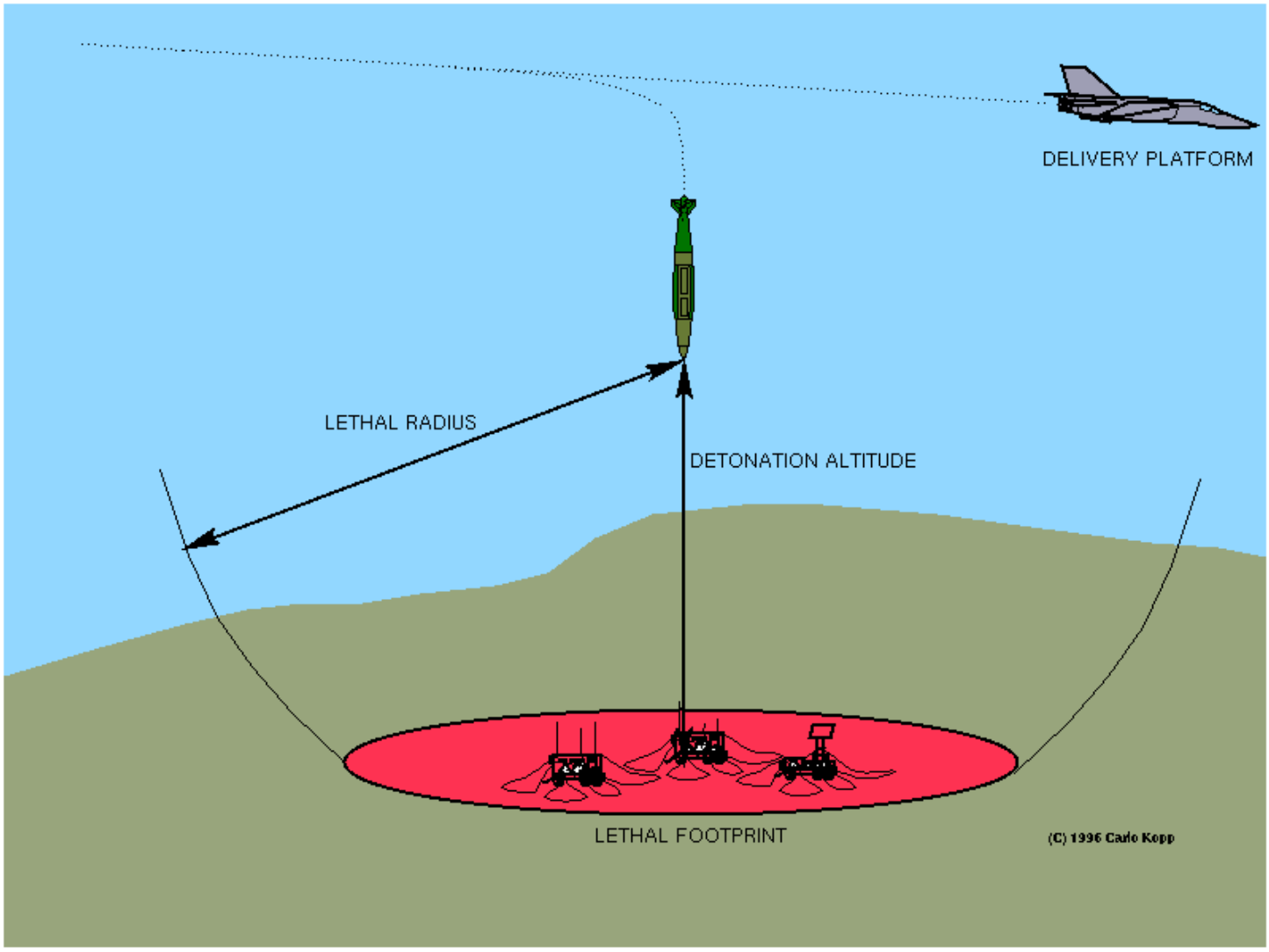


FIG.7 LETHAL FOOTPRINT OF LOW FREQUENCY E- BOMB IN RELATION TO ALTITUDE

The practical constraint is that it may be difficult to produce an efficient high power circularly polarised antenna design which is compact and performs over a wide band. Some work therefore needs to be done on tapered helix or conical spiral type antennas capable of handling high power levels, and a suitable interface to a Vircator with multiple extraction ports must devised. A possible implementation is depicted in Fig.5. In this arrangement, power is coupled from the tube by stubs which directly feed a multi-filar conical helix antenna. An implementation of this scheme would need to address the specific requirements of bandwidth, beamwidth, efficiency of coupling from the tube, while delivering circularly polarised radiation.

Another aspect of electromagnetic bomb lethality is its detonation altitude, and by varying the detonation altitude, a tradeoff may be achieved between the size of the lethal footprint and the intensity of the electromagnetic field in that footprint. This provides the option of sacrificing weapon coverage to achieve kills against targets of greater electromagnetic hardness, for a given bomb size (Fig.7, 8). This is not unlike the use of airburst explosive devices.

In summary, lethality is maximised by maximising power output and the efficiency of energy transfer from the weapon to the target set. Microwave weapons offer the ability to focus nearly all of their energy output into the lethal footprint, and offer the ability to exploit a wider range of coupling modes. Therefore, microwave bombs are the preferred choice.

5. Targeting Electromagnetic Bombs

The task of identifying targets for attack with electromagnetic bombs can be complex. Certain categories of target will be very easy to identify and engage. Buildings housing government offices and thus computer equipment, production facilities, military bases and known radar sites and communications nodes are all targets which can be readily identified through conventional photographic, satellite, imaging radar, electronic reconnaissance and humint operations. These targets are typically geographically fixed and thus may be attacked providing that the aircraft can penetrate to weapon release range. With the accuracy inherent in GPS/inertially guided weapons, the electromagnetic bomb can be programmed to detonate at the optimal

position to inflict a maximum of electrical damage.

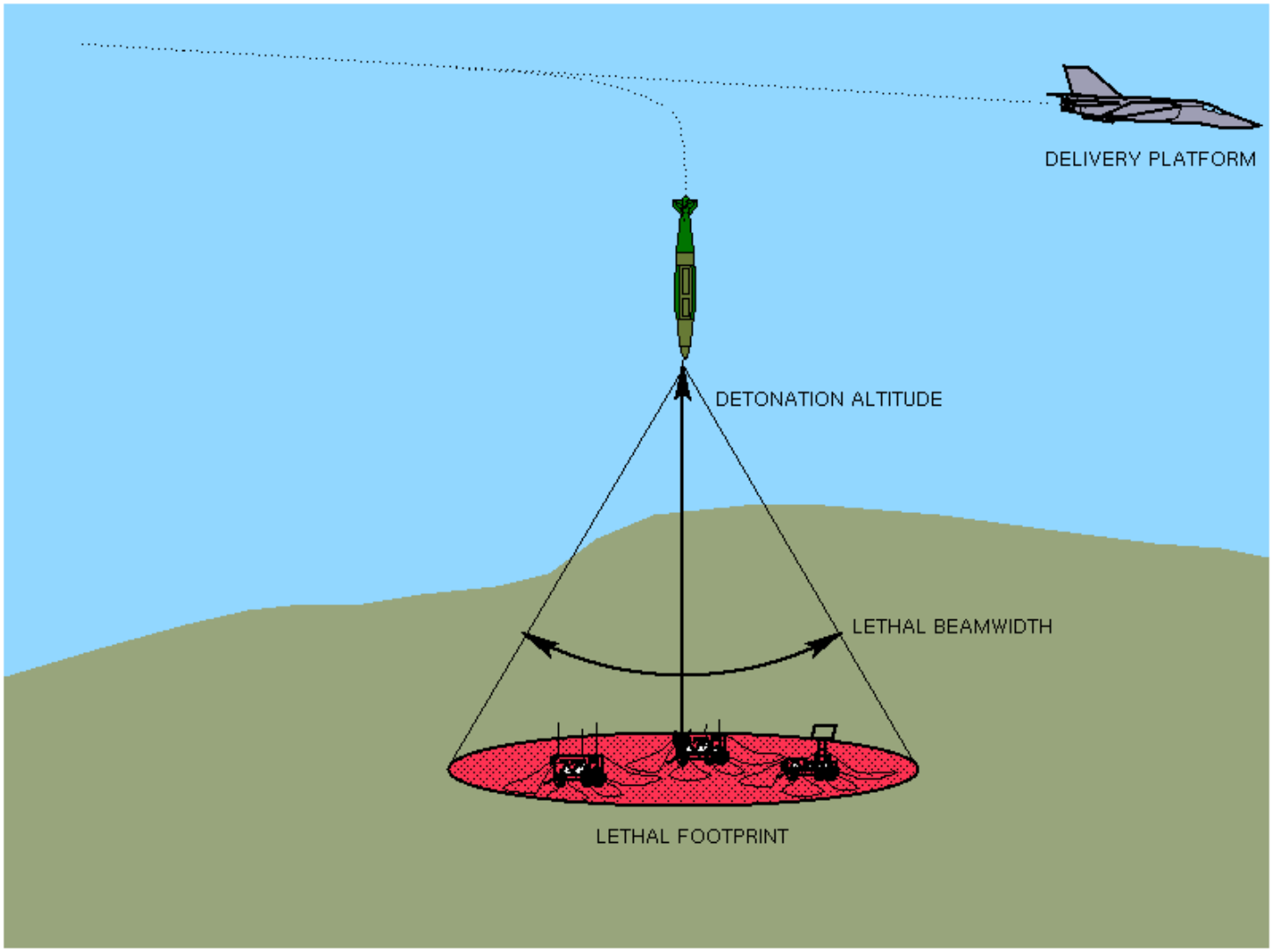


FIG.8 LETHAL FOOTPRINT OF A HPM E-BOMB IN RELATION TO ALTITUDE

Mobile and camouflaged targets which radiate overtly can also be readily engaged. Mobile and relocatable air defence equipment, mobile communications nodes and naval vessels are all good examples of this category of target. While radiating, their positions can be precisely tracked with suitable Electronic Support Measures (ESM) and Emitter Locating Systems (ELS) carried either by the launch platform or a remote surveillance platform. In the latter instance target coordinates can be continuously datalinked to the launch platform. As most such targets move relatively slowly, they are unlikely to escape the footprint of the electromagnetic bomb during the weapon's flight time.

Mobile or hidden targets which do not overtly radiate may present a problem, particularly should conventional means of targeting be employed. A technical solution to this problem does however exist, for many types of target. This solution is the detection and tracking of Unintentional Emission (UE) [HERSKOWITZ96]. UE has attracted most attention in the context of TEMPEST [3] surveillance, where transient emanations leaking out from equipment due poor shielding can be detected and in many instances demodulated to recover useful intelligence. Termed Van Eck radiation [VECK85], such emissions can only be suppressed by rigorous shielding and emission control techniques, such as are employed in TEMPEST rated equipment.

Whilst the demodulation of UE can be a technically difficult task to perform well, in the context of targeting electromagnetic bombs this problem does not arise. To target such an emitter for attack requires only the ability to identify the type of emission and thus target type, and to isolate its position with sufficient accuracy to deliver the bomb. Because the emissions from computer monitors, peripherals, processor equipment, switchmode power supplies, electrical motors, internal combustion engine ignition systems, variable duty cycle electrical power controllers (thyristor or triac based), superheterodyne receiver local oscillators and computer networking cables are all distinct in their frequencies and modulations, a suitable Emitter Locating

System can be designed to detect, identify and track such sources of emission.

A good precedent for this targeting paradigm exists. During the SEA (Vietnam) conflict the United States Air Force (USAF) operated a number of night interdiction gunships which used direction finding receivers to track the emissions from vehicle ignition systems. Once a truck was identified and tracked, the gunship would engage it [4].

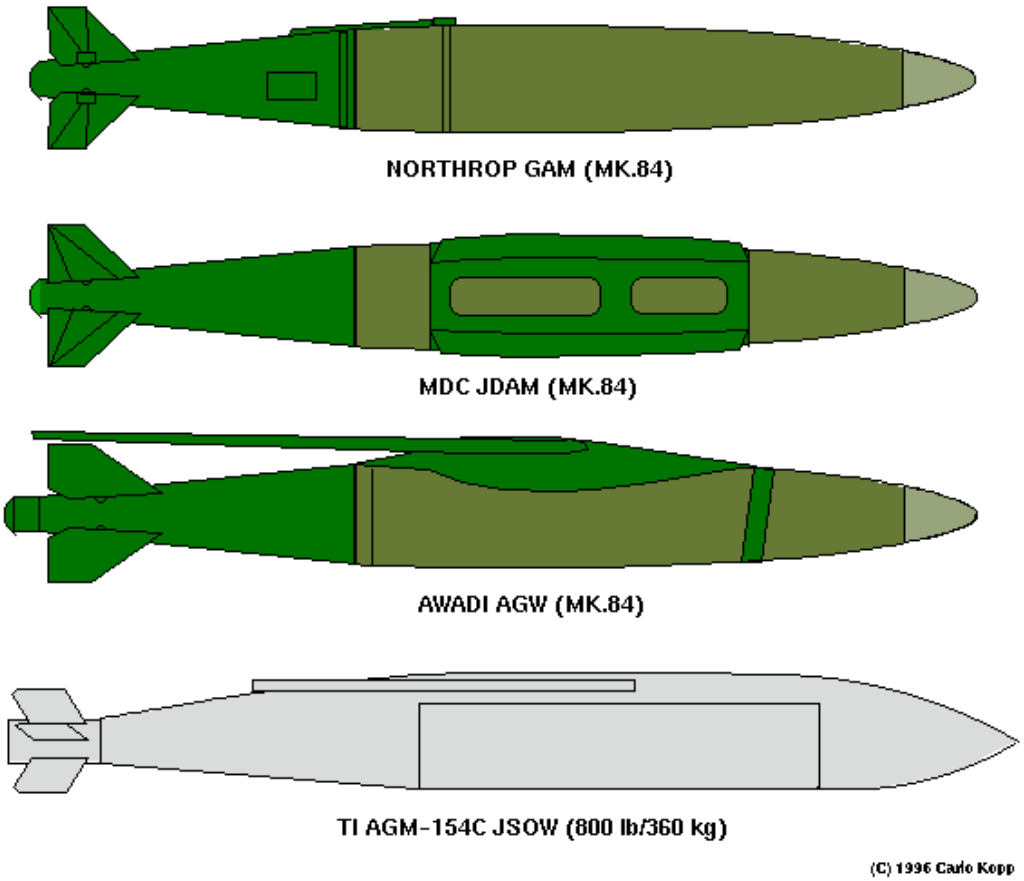


FIG.9 GPS GUIDED BOMB/GLIDEBOMB KITS

Because UE occurs at relatively low power levels, the use of this detection method prior to the outbreak of hostilities can be difficult, as it may be necessary to overfly hostile territory to find signals of usable intensity [5]. The use of stealthy reconnaissance aircraft or long range, stealthy Unmanned Aerial Vehicles (UAV) may be required. The latter also raises the possibility of autonomous electromagnetic warhead armed expendable UAVs, fitted with appropriate homing receivers. These would be programmed to loiter in a target area until a suitable emitter is detected, upon which the UAV would home in and expend itself against the target.

6. The Delivery of Conventional Electromagnetic Bombs

As with explosive warheads, electromagnetic warheads will occupy a volume of physical space and will also have some given mass (weight) determined by the density of the internal hardware. Like explosive warheads, electromagnetic warheads may be fitted to a range of delivery vehicles.

Known existing applications [6] involve fitting an electromagnetic warhead to a cruise missile airframe. The choice of a cruise missile airframe will restrict the weight of the weapon to about 340 kg (750 lb), although some sacrifice in airframe fuel capacity could see this size increased. A limitation in all such applications is the need to carry an electrical energy storage device, eg a battery, to provide the current used to charge the capacitors used to prime the FCG prior to its discharge. Therefore the available payload capacity will be split between the electrical storage and the weapon itself.

In wholly autonomous weapons such as cruise missiles, the size of the priming current source and its battery may well impose important limitations on weapon capability. Air delivered bombs, which have a flight time between tens of seconds to minutes, could be built to exploit the launch aircraft's power systems. In such a bomb design, the bomb's capacitor bank can be charged by the launch aircraft enroute to target, and after release a much smaller onboard power supply could be used to maintain the charge in the priming source prior to weapon initiation.

An electromagnetic bomb delivered by a conventional aircraft [7] can offer a much better ratio of electromagnetic device mass to total bomb mass, as most of the bomb mass can be dedicated to the electromagnetic device installation itself. It follows therefore, that for a given technology an electromagnetic bomb of identical mass to a electromagnetic warhead equipped missile can have a much greater lethality, assuming equal accuracy of delivery and technologically similar electromagnetic device design.

A missile borne electromagnetic warhead installation will comprise the electromagnetic device, an electrical energy converter, and an onboard storage device such as a battery. As the weapon is pumped, the battery is drained. The electromagnetic device will be detonated by the missile's onboard fusing system. In a cruise missile, this will be tied to the navigation system; in an anti-shipping missile the radar seeker and in an air-to-air missile, the proximity fusing system. The warhead fraction (ie ratio of total payload (warhead) mass to launch mass of the weapon) will be between 15% and 30% [8].

An electromagnetic bomb warhead will comprise an electromagnetic device, an electrical energy converter and a energy storage device to pump and sustain the electromagnetic device charge after separation from the delivery platform. Fusing could be provided by a radar altimeter fuse to airburst the bomb, a barometric fuse or in GPS/inertially guided bombs, the navigation system. The warhead fraction could be as high as 85%, with most of the usable mass occupied by the electromagnetic device and its supporting hardware.

Due to the potentially large lethal radius of an electromagnetic device, compared to an explosive device of similar mass, standoff delivery would be prudent. Whilst this is an inherent characteristic of weapons such as cruise missiles, potential applications of these devices to glidebombs, anti-shipping missiles and air-to-air missiles would dictate fire and forget guidance of the appropriate variety, to allow the launching aircraft to gain adequate separation of several miles before warhead detonation.

The recent advent of GPS satellite navigation guidance kits for conventional bombs and glidebombs has provided the optimal means for cheaply delivering such weapons. While GPS guided weapons without differential GPS enhancements may lack the pinpoint accuracy of laser or television guided munitions, they are still quite accurate (CEP \(~~ 40 ft) and importantly, cheap, autonomous all weather weapons.

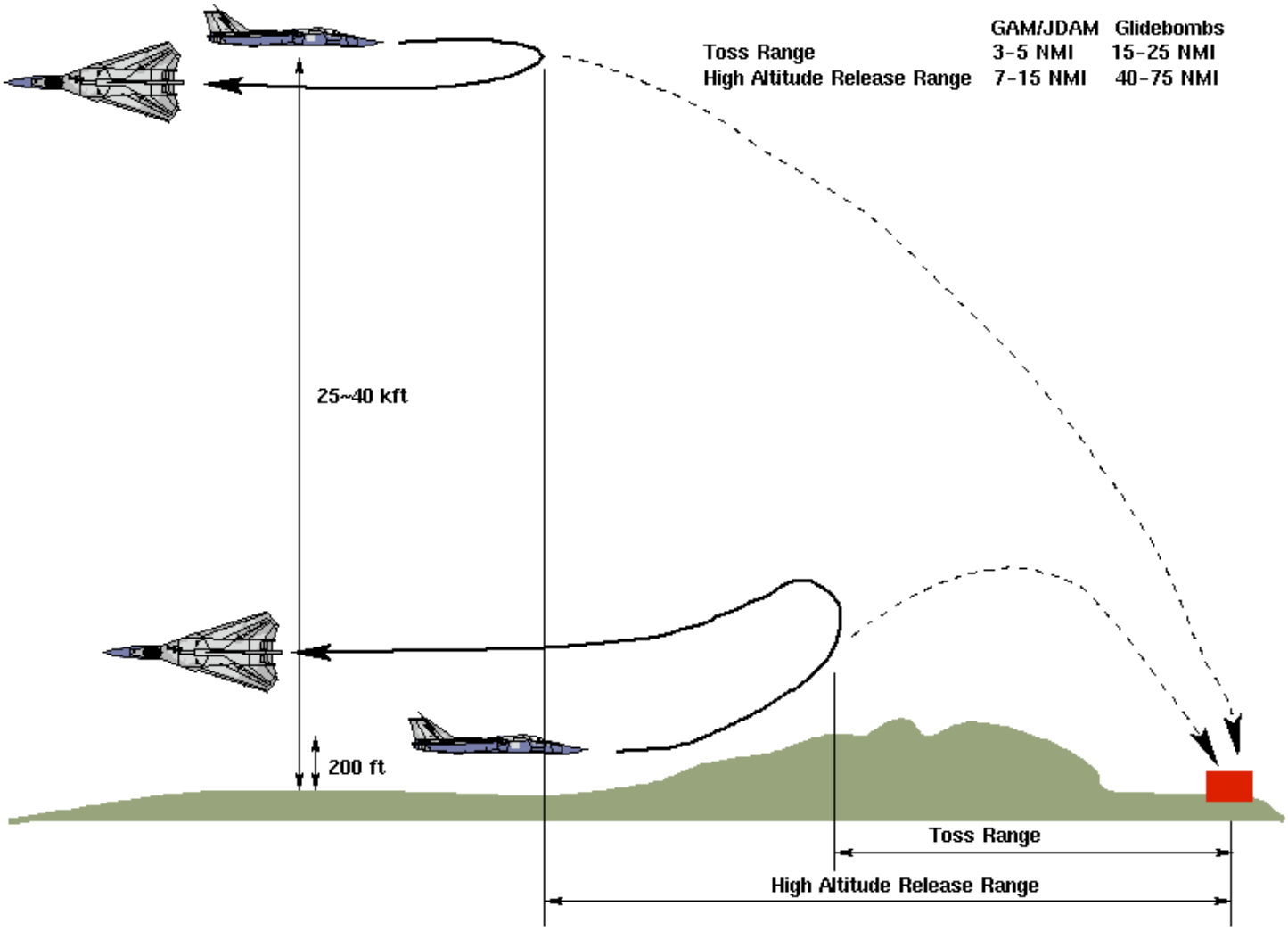


FIG.10 DELIVERY PROFILES FOR GPS/INERTIAL GUIDED WEAPONS

The USAF has recently deployed the Northrop GAM (GPS Aided Munition) on the B-2 bomber [NORTHROP95], and will by the end of the decade deploy the GPS/inertially guided GBU-29/30 JDAM (Joint Direct Attack Munition)[MDC95] and the AGM-154 JSOW (Joint Stand Off Weapon) [PERGLER94] glidebomb. Other countries are also developing this technology, the Australian BAeA AGW (Agile Glide Weapon) glidebomb achieving a glide range of about 140 km (75 nmi) when launched from altitude [KOPP96].

The importance of glidebombs as delivery means for HPM warheads is threefold. Firstly, the glidebomb can be released from outside effective radius of target air defences, therefore minimising the risk to the launch aircraft. Secondly, the large standoff range means that the aircraft can remain well clear of the bomb's effects. Finally the bomb's autopilot may be programmed to shape the terminal trajectory of the weapon, such that a target may be engaged from the most suitable altitude and aspect.

A major advantage of using electromagnetic bombs is that they may be delivered by any tactical aircraft with a nav-attack system capable of delivering GPS guided munitions. As we can expect GPS guided munitions to be become the standard weapon in use by Western air forces by the end of this decade, every aircraft capable of delivering a standard guided munition also becomes a potential delivery vehicle for a electromagnetic bomb. Should weapon ballistic properties be identical to the standard weapon, no software changes to the aircraft would be required.

Because of the simplicity of electromagnetic bombs in comparison with weapons such as Anti Radiation Missiles (ARM), it is not unreasonable to expect that these should be both cheaper to manufacture, and easier to support in the field, thus allowing for more substantial weapon stocks. In turn this makes saturation attacks a much more viable proposition.

In this context it is worth noting that the USAF's possesion of the JDAM capable F-117A and B-2A will provide the capability to deliver E-bombs against arbitrary high value targets with virtual impunity. The ability of a B-2A to deliver up to sixteen GAM/JDAM fitted E-bomb warheads with a 20 ft class CEP would allow a small number of such aircraft to deliver a decisive blow against key strategic, air defence and theatre targets. A strike and electronic combat capable derivative of the F-22 would also be a viable delivery platform for an E-bomb/JDAM. With its superb radius, low signature and supersonic cruise capability an RFB-22 could attack air defence sites, C3I sites, airbases and strategic targets with E-bombs, achieving a significant shock

effect. A good case may be argued for the whole F-22 build to be JDAM/E-bomb capable, as this would allow the USAF to apply the maximum concentration of force against arbitrary air and surface targets during the opening phase of an air campaign.

7. Defence Against Electromagnetic Bombs

The most effective defence against electromagnetic bombs is to prevent their delivery by destroying the launch platform or delivery vehicle, as is the case with nuclear weapons. This however may not always be possible, and therefore systems which can be expected to suffer exposure to the electromagnetic weapons effects must be electromagnetically hardened.

The most effective method is to wholly contain the equipment in an electrically conductive enclosure, termed a Faraday cage, which prevents the electromagnetic field from gaining access to the protected equipment. However, most such equipment must communicate with and be fed with power from the outside world, and this can provide entry points via which electrical transients may enter the enclosure and effect damage. While optical fibres address this requirement for transferring data in and out, electrical power feeds remain an ongoing vulnerability.

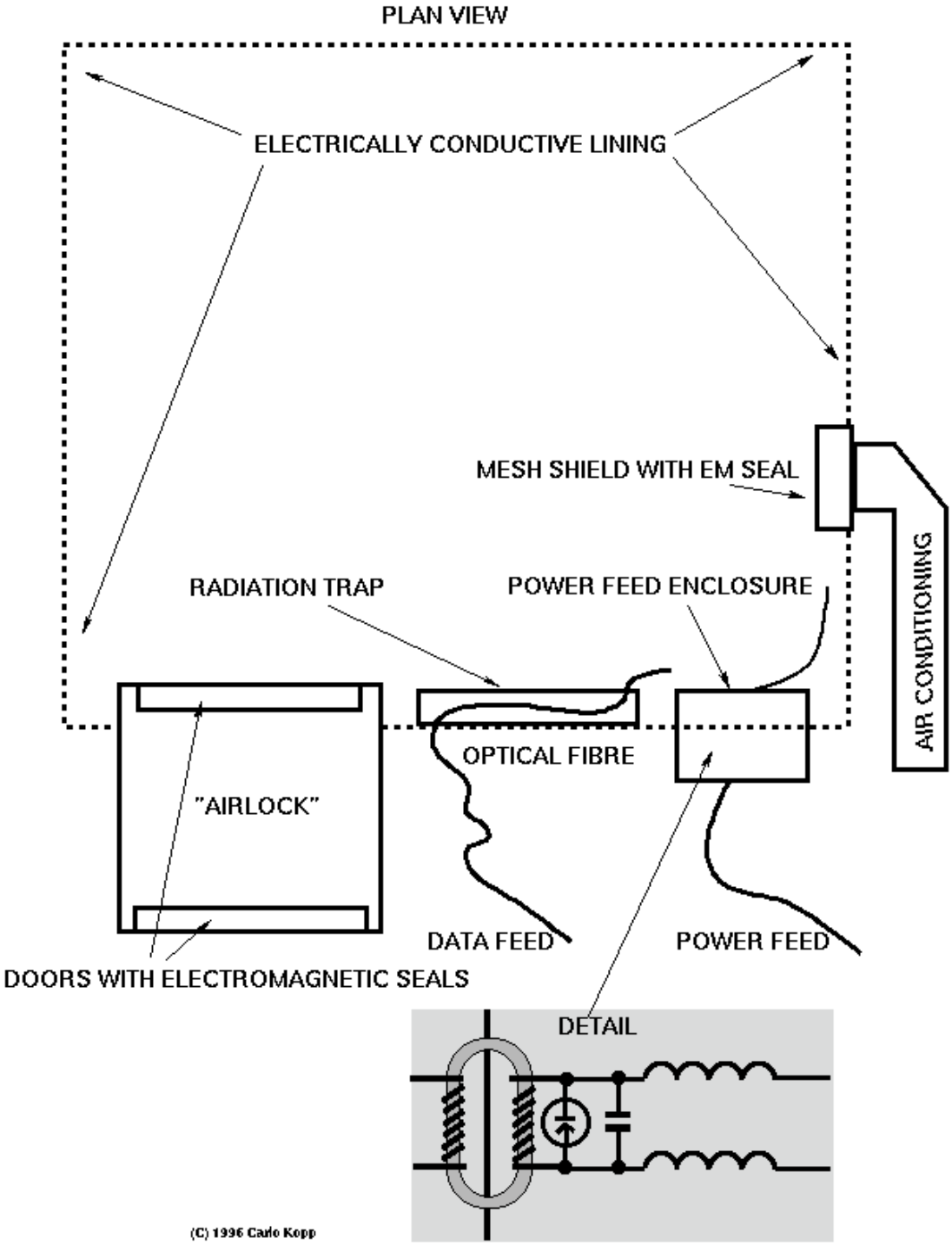


FIG.11 COMPUTER ROOM HARDENED AGAINST EM ATTACK

Where an electrically conductive channel must enter the enclosure, electromagnetic arresting devices must be fitted. A range of devices exist, however care must be taken in determining their parameters to ensure that they can deal with the rise time and strength of electrical transients produced by electromagnetic devices. Reports from the US [9] indicate that hardening measures attuned to the behaviour of nuclear EMP bombs do not perform well when dealing with some conventional microwave electromagnetic device designs.

It is significant that hardening of systems must be carried out at a system level, as electromagnetic damage to any single element of a complex system could inhibit the function of the whole system. Hardening new build equipment and systems will add a substantial cost burden. Older equipment and systems may be impossible to harden properly and may require complete

replacement. In simple terms, hardening by design is significantly easier than attempting to harden existing equipment.

An interesting aspect of electrical damage to targets is the possibility of wounding semiconductor devices thereby causing equipment to suffer repetitive intermittent faults rather than complete failures. Such faults would tie down considerable maintenance resources while also diminishing the confidence of the operators in the equipment's reliability. Intermittent faults may not be possible to repair economically, thereby causing equipment in this state to be removed from service permanently, with considerable loss in maintenance hours during damage diagnosis. This factor must also be considered when assessing the hardness of equipment against electromagnetic attack, as partial or incomplete hardening may in this fashion cause more difficulties than it would solve. Indeed, shielding which is incomplete may resonate when excited by radiation and thus contribute to damage inflicted upon the equipment contained within it.

Other than hardening against attack, facilities which are concealed should not radiate readily detectable emissions. Where radio frequency communications must be used, low probability of intercept (ie spread spectrum) techniques should be employed exclusively to preclude the use of site emissions for electromagnetic targeting purposes [DIXON84]. Appropriate suppression of UE is also mandatory.

Communications networks for voice, data and services should employ topologies with sufficient redundancy and failover mechanisms to allow operation with multiple nodes and links inoperative. This will deny a user of electromagnetic bombs the option of disabling large portions if not the whole of the network by taking down one or more key nodes or links with a single or small number of attacks.

8. Limitations of Electromagnetic Bombs

The limitations of electromagnetic weapons are determined by weapon implementation and means of delivery. Weapon implementation will determine the electromagnetic field strength achievable at a given radius, and its spectral distribution. Means of delivery will constrain the accuracy with which the weapon can be positioned in relation to the intended target. Both constrain lethality.

In the context of targeting military equipment, it must be noted that thermionic technology (ie vacuum tube equipment) is substantially more resilient to the electromagnetic weapons effects than solid state (ie transistor) technology. Therefore a weapon optimised to destroy solid state computers and receivers may cause little or no damage to a thermionic technology device, for instance early 1960s Soviet military equipment. Therefore a hard electrical kill may not be achieved against such targets unless a suitable weapon is used.

This underscores another limitation of electromagnetic weapons, which is the difficulty in kill assessment. Radiating targets such as radars or communications equipment may continue to radiate after an attack even though their receivers and data processing systems have been damaged or destroyed. This means that equipment which has been successfully attacked may still appear to operate. Conversely an opponent may shut down an emitter if attack is imminent and the absence of emissions means that the success or failure of the attack may not be immediately apparent.

Assessing whether an attack on a non radiating emitter has been successful is more problematic. A good case can be made for developing tools specifically for the purpose of analysing unintended emissions, not only for targeting purposes, but also for kill assessment.

An important factor in assessing the lethal coverage of an electromagnetic weapon is atmospheric propagation. While the relationship between electromagnetic field strength and distance from the weapon is one of an inverse square law in free space, the decay in lethal effect with increasing distance within the atmosphere will be greater due quantum physical absorption effects [10]. This is particularly so at higher frequencies, and significant absorption peaks due water vapour and oxygen exist at frequencies above 20 GHz. These will therefore contain the effect of HPM weapons to shorter radii than are ideally achievable in the K and L frequency bands.

Means of delivery will limit the lethality of an electromagnetic bomb by introducing limits to the weapon's size and the accuracy of its delivery. Should the delivery error be of the order of the weapon's lethal radius for a given detonation altitude, lethality will be significantly diminished. This is of particular importance when assessing the lethality of unguided electromagnetic bombs, as delivery errors will be more substantial than those experienced with guided weapons such as GPS guided bombs.

Therefore accuracy of delivery and achievable lethal radius must be considered against the allowable collateral damage for the chosen target. Where collateral electrical damage is a consideration, accuracy of delivery and lethal radius are key parameters. An inaccurately delivered weapon of large lethal radius may be unusable against a target should the likely collateral electrical damage be beyond acceptable limits. This can be a major issue for users constrained by treaty provisions on collateral damage [AAP1003].

9. The Proliferation of Electromagnetic Bombs

At the time of writing, the United States and the CIS are the only two nations with the established technology base and the depth of specific experience to design weapons based upon this technology. However, the relative simplicity of the FCG and the Vircator suggests that any nation with even a 1940s technology base, once in possession of engineering drawings and specifications for such weapons, could manufacture them.

As an example, the fabrication of an effective FCG can be accomplished with basic electrical materials, common plastic

explosives such as C-4 or Semtex, and readily available machine tools such as lathes and suitable mandrels for forming coils. Disregarding the overheads of design, which do not apply in this context, a two stage FCG could be fabricated for a cost as low as $1,000-2,000, at Western labour rates [REINOVSKY85]. This cost could be even lower in a Third World or newly industrialised economy.

While the relative simplicity and thus low cost of such weapons can be considered of benefit to First World nations intending to build viable war stocks or maintain production in wartime, the possibility of less developed nations mass producing such weapons is alarming. The dependence of modern economies upon their information technology infrastructure makes them highly vulnerable to attack with such weapons, providing that these can be delivered to their targets.

Of major concern is the vulnerability resulting from increasing use of communications and data communications schemes based upon copper cable media. If the copper medium were to be replaced en masse with optical fibre in order to achieve higher bandwidths, the communications infrastructure would become significantly more robust against electromagnetic attack as a result. However, the current trend is to exploit existing distribution media such as cable TV and telephone wiring to provide multiple Megabit/s data distribution (eg cable modems, ADSL/HDSL/VDSL) to premises. Moreover, the gradual replacement of coaxial Ethernet networking with 10-Base-T twisted pair equipment has further increased the vulnerability of wiring systems inside buildings. It is not unreasonable to assume that the data and services communications infrastructure in the West will remain a "soft" electromagnetic target in the forseeable future.

At this time no counter-proliferation regimes exist. Should treaties be agreed to limit the proliferation of electromagnetic weapons, they would be virtually impossible to enforce given the common availability of suitable materials and tools.

With the former CIS suffering significant economic difficulties, the possibility of CIS designed microwave and pulse power technology leaking out to Third World nations or terrorist organisations should not be discounted. The threat of electromagnetic bomb proliferation is very real.

10. A Doctrine for the Use of Conventional Electromagnetic Bombs

A fundamental tenet of IW is that complex organisational systems such as governments, industries and military forces cannot function without the flow of information through their structures. Information flows within these structures in several directions, under typical conditions of function. A trivial model for this function would see commands and directives flowing outward from a central decisionmaking element, with information about the state of the system flowing in the opposite direction. Real systems are substantially more complex.

This is of military significance because stopping this flow of information will severely debilitate the function of any such system. Stopping the outward flow of information produces paralysis, as commands cannot reach the elements which are to execute them. Stopping the inward flow of information isolates the decisionmaking element from reality, and thus severely inhibits its capacity to make rational decisions which are sensitive to the currency of information at hand.

The recent evolution of strategic (air) warfare indicates a growing trend toward targeting strategies which exploit this most fundamental vulnerability of any large and organised system [11]. The Desert Storm air war of 1991 is a good instance, with a substantial effort expended against such targets. Indeed, the model used for modern strategic air attack places leadership and its supporting communications in the position of highest targeting priority [WARDEN95]. No less importantly, modern Electronic Combat concentrates upon the disruption and destruction of communications and information gathering sensors used to support military operations. Again the Desert Storm air war provides a good illustration of the application of this method.

A strategy which stresses attack upon the information processing and communications elements of the systems which it is targeting offers a very high payoff, as it will introduce an increasing level of paralysis and disorientation within its target. Electromagnetic bombs are a powerful tool in the implementation of such a strategy.

10.1 Electronic Combat Operations using Electromagnetic Bombs

The central objective of Electronic Combat (EC) operations is the command of the electromagnetic spectrum, achieved by soft and hard kill means [12] against the opponent's electronic assets. The underlying objective of commanding the electromagnetic spectrum is to interrupt or substantially reduce the flow of information through the opponent's air defence system, air operations environment and between functional elements of weapon systems.

In this context the ability of electromagnetic bombs to achieve kills against a wide range of target types allows their general application to the task of inflicting attrition upon an opponent's electronic assets, be they specialised air defence assets or more general Command-Control-Communications (C3) and other military assets.

Electromagnetic bombs can be a means of both soft and hard electrical kill, subject to the lethality of the weapon and the hardness of its target. A hard electrical kill by means of an electromagnetic device will be achieved in those instances where such severe electrical damage is achieved against a target so as to require the replacement of most if not all of its internal electronics.

Electronic combat operations using electromagnetic devices involve the use of these to attack radar, C3 and air defence weapon systems. These should always be attacked initially with an electromagnetic weapon to achieve soft or hard electrical kills, followed up by attack with conventional munitions to preclude possible repair of disabled assets at a later time. As with conventional SEAD operations, the greatest payoff will be achieved by using electromagnetic weapons against systems of

strategic importance first, followed in turn by those of operational and tactical importance [KOPP92].

In comparison with an AntiRadiation Missile (ARM - a missile which homes on the emissions from a threat radar), the established and specialised tool in the conduct of SEAD operations, an electromagnetic bomb can achieve kills against multiple targets of diverse types within its lethal footprint. In this respect an electromagnetic device may be described as a Weapon of Electrical Mass Destruction (WEMD). Therefore electromagnetic weapons are a significant force multiplier in electronic combat operations.

A conventional electronic combat campaign, or intensive electronic combat operations, will initially concentrate on saturating the opponent's electronic defences, denying information and inflicting maximum attrition upon electronic assets. The force multiplication offered by electromagnetic weapons vastly reduces the number of air assets required to inflict substantial attrition, and where proper electronic reconnaissance has been carried out beforehand, also reduces the need for specialised assets such as ARM firing aircraft equipped with costly emitter locating systems.

The massed application of electromagnetic bombs in the opening phase of an electronic battle will allow much faster attainment of command of the electromagnetic spectrum, as it will inflict attrition upon electronic assets at a much faster rate than possible with conventional means.

Whilst the immaturity of conventional electromagnetic weapons precludes an exact analysis of the scale of force multiplication achievable, it is evident that a single aircraft carrying an electromagnetic bomb capable of concurrently disabling a SAM site with its colocated acquisition radar and supporting radar directed AAA weapons, will have the potency of the several ARM firing and support jamming aircraft required to accomplish the same result by conventional means. This and the ability of multirole tactical aircraft to perform this task allows for a much greater concentration of force in the opening phase of the battle, for a given force size.

In summary the massed application of electromagnetic weapons to Electronic Combat operations will provide for a much faster rate of attrition against hostile electronic assets, achievable with a significantly reduced number of specialised and multirole air assets [13]. This will allow even a modestly sized force to apply overwhelming pressure in the initial phase of an electronic battle, and therefore achieve command of the electromagnetic spectrum in a significantly shorter time than by conventional means.

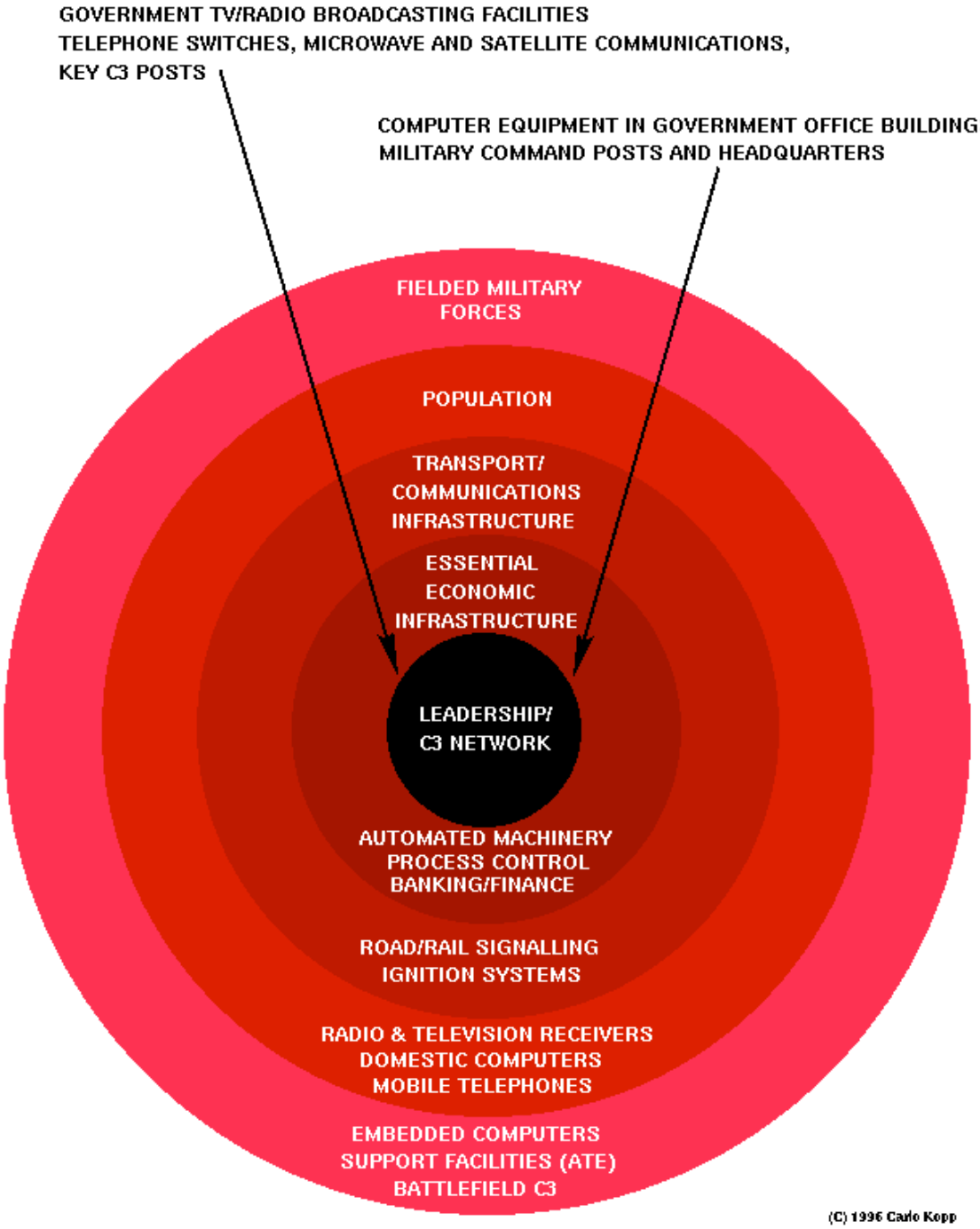


FIG.12 WARDEN'S "FIVE RINGS" STRATEGIC AIR ATTACK MODEL
IN THE CONTEXT OF ELECTROMAGNETICALLY VULNERABLE TARGET SETS

10.2. Strategic Air Attack Operations using Electromagnetic Bombs

The modern approach to strategic air warfare reflects in many respects aspects of the IW model, in that much effort is expended in disabling an opponent's fundamental information processing infrastructure. Since we however are yet to see a systematic IW doctrine which has been tested in combat, this paper will approach the subject from a more conservative viewpoint and use established strategic doctrine.

Modern strategic air attack theory is based upon Warden's Five Rings model [WARDEN95], which identifies five centres of gravity in a nation's warfighting capability. In descending order of importance, these are the nation's leadership and supporting C3 system, its essential economic infrastructure, its transportation network, its population and its fielded military forces.

Electromagnetic weapons may be productively used against all elements in this model, and provide a particularly high payoff

when applied against a highly industrialised and geographically concentrated opponent. Of particular importance in the context of strategic air attack, is that while electromagnetic weapons are lethal to electronics, they have little if any effect on humans. This is a characteristic which is not shared with established conventional and nuclear weapons.

This selectivity in lethal effect makes electromagnetic weapons far more readily applicable to a strategic air attack campaign, and reduces the internal political pressure which is experienced by the leadership of any democracy which must commit to warfare. An opponent may be rendered militarily, politically and economically ineffective with little if any loss in human life.

The innermost ring in the Warden model essentially comprises government bureaucracies and civilian and military C3 systems. In any modern nation these are heavily dependent upon the use of computer equipment and communications equipment. What is of key importance at this time is an ongoing change in the structure of computing facilities used in such applications, as these are becoming increasingly decentralised. A modern office environment relies upon a large number of small computers, networked to interchange information, in which respect it differs from the traditional model of using a small number of powerful central machines.

This decentralisation and networking of information technology systems produces a major vulnerability to electromagnetic attack. Whereas a small number of larger computers could be defended against electromagnetic attack by the use of electromagnetic hardened computer rooms, a large distributed network cannot. Moreover, unless optical fibre networking is used, the networking cables are themselves a medium via which electromagnetic effects can be efficiently propagated throughout the network, to destroy machines. Whilst the use of distributed computer networks reduces vulnerability to attack by conventional munitions, it increases vulnerability to attack by electromagnetic weapons.

Selective targeting of government buildings with electromagnetic weapons will result in a substantial reduction in a government's ability to handle and process information. The damage inflicted upon information records may be permanent, should inappropriate backup strategies have been used to protect stored data. It is reasonable to expect most data stored on machines which are affected will perish with the host machine, or become extremely difficult to recover from damaged storage devices.

The cost of hardening existing computer networks is prohibitive, as is the cost of replacement with hardened equipment. Whilst the use of hardened equipment for critical tasks would provide some measure of resilience, the required discipline in the handling of information required to implement such a scheme renders its utility outside of military organisations questionable. Therefore the use of electromagnetic weapons against government facilities offers an exceptionally high payoff.

Other targets which fall into the innermost ring may also be profitably attacked. Satellite link and importantly control facilities are vital means of communication as well as the primary interface to military and commercial reconnaissance satellites. Television and radio broadcasting stations, one of the most powerful tools of any government, are also vulnerable to electromagnetic attack due the very high concentration of electronic equipment in such sites. Telephone exchanges, particularly later generation digital switching systems, are also highly vulnerable to appropriate electromagnetic attack.

In summary the use of electromagnetic weapons against leadership and C3 targets is highly profitable, in that a modest number of weapons appropriately used can introduce the sought state of strategic paralysis, without the substantial costs incurred by the use of conventional munitions to achieve the same effect.

Essential economic infrastructure is also vulnerable to electromagnetic attack. The finance industry and stock markets are almost wholly dependent upon computers and their supporting communications. Manufacturing, chemical, petroleum product industries and metallurgical industries rely heavily upon automation which is almost universally implemented with electronic PLC (Programmable Logic Controller) systems or digital computers. Furthermore, most sensors and telemetry devices used are electrical or electronic.

Attacking such economic targets with electromagnetic weapons will halt operations for the time required to either repair the destroyed equipment, or to reconfigure for manual operation. Some production processes however require automated operation, either because hazardous conditions prevent human intervention, or the complexity of the control process required cannot be carried out by a human operator in real time. A good instance are larger chemical, petrochemical and oil/gas production facilities. Destroying automated control facilities will therefore result in substantial loss of production, causing shortages of these vital materials.

Manufacturing industries which rely heavily upon robotic and semiautomatic machinery, such as the electronics, computer and electrical industry, precision machine industry and aerospace industries, are all key assets in supporting a military capability. They are all highly vulnerable to electromagnetic attack. Whilst material processing industries may in some instances be capable of function with manual process control, the manufacturing industries are almost wholly dependent upon their automated machines to achieve any useful production output.

Historical experience [14] suggests that manufacturing industries are highly resilient to air attack as production machinery is inherently mechanically robust and thus a very high blast overpressure is required to destroy it. The proliferation of electronic and computer controlled machinery has produced a major vulnerability, for which historical precedent does not exist. Therefore it will be necessary to reevaluate this orthodoxy in targeting strategy.

The finance industry and stock markets are a special case in this context, as the destruction of their electronic infrastructure can yield, unlike manufacturing industries, much faster economic dislocation. This can in turn produce large systemic effects across a whole economy, including elements which are not vulnerable to direct electromagnetic attack. This may be of particular relevance when dealing with an opponent which does not have a large and thus vulnerable manufacturing economy. Nations which rely on agriculture, mining or trade for a large proportion of the their gross domestic product are prime candidates for

electromagnetic attack on their finance industry and stock markets. Since the latter are usually geographically concentrated and typically electromagnetically "soft" targets, they are highly vulnerable.

In summary there is a large payoff in striking at economic essentials with electromagnetic weapons, particularly in the opening phase of a strategic air attack campaign, as economic activity may be halted or reduced with modest expenditure of the attacker's resources. An important caveat is that centres of gravity within the target economy must be properly identified and prioritised for strikes to ensure that maximum effect is achieved as quickly as possible.

Transport infrastructure is the third ring in the Warden model, and also offers some useful opportunities for the application of electromagnetic weapons. Unlike the innermost rings, the concentration of electronic and computer equipment is typically much lower, and therefore considerable care must be taken in the selection of targets.

Railway and road signalling systems, where automated, are most vulnerable to electromagnetic attack on their control centres. This could be used to produce traffic congestion by preventing the proper scheduling of rail traffic, and disabling road traffic signalling, although the latter may not yield particularly useful results.

Significantly, most modern automobiles and trucks use electronic ignition systems which are known to be vulnerable to electromagnetic weapons effects, although opportunities to find such concentrations so as to allow the profitable use of an electromagnetic bomb may be scarce.

The population of the target nation is the fourth ring in the Warden model, and its morale is the object of attack. The morale of the population will be affected significantly by the quality and quantity of the government propaganda it is subjected to, as will it be affected by living conditions.

Using electromagnetic weapons against urban areas provides the opportunity to prevent government propaganda from reaching the population via means of mass media, through the damaging or destruction of all television and radio receivers within the footprint of the weapon. Whether this is necessary, given that broadcast facilities may have already been destroyed, is open to discussion. Arguably it may be counterproductive, as it will prevent the target population from being subjected to friendly means of psychological warfare such as propaganda broadcasts.

The use of electromagnetic weapons against a target population is therefore an area which requires requires careful consideration in the context of the overall IW campaign strategy. If useful objectives can be achieved by isolating the population from government propaganda, then the population is a valid target for electromagnetic attack. Forces constrained by treaty obligations will have to reconcile this against the applicable regulations relating to denial of services to non-combatants [AAP1003].

The outermost and last ring in the Warden model are the fielded military forces. These are by all means a target vulnerable to electromagnetic attack, and C3 nodes, fixed support bases as well as deployed forces should be attacked with electromagnetic devices. Fixed support bases which carry out depot level maintenance on military equipment offer a substantial payoff, as the concentration of computers in both automatic test equipment and administrative and logistic support functions offers a good return per expended weapon.

Any site where more complex military equipment is concentrated should be attacked with electromagnetic weapons to render the equipment unservicable and hence reduce the fighting capability, and where possible also mobility of the targeted force. As discussed earlier in the context of Electronic Combat, the ability of an electromagnetic weapon to achieve hard electrical kills against any non-hardened targets within its lethal footprint suggests that some target sites may only require electromagnetic attack to render them both undefended and non-operational. Whether to expend conventional munitions on targets in this state would depend on the immediate military situation.

In summary the use of electromagnetic weapons in strategic air attack campaign offers a potentially high payoff, particularly when applied to leadership, C3 and vital economic targets, all of which may be deprived of much of their function for substantial periods of time. The massed application of electromagnetic weapons in the opening phase of the campaign would introduce paralysis within the government, deprived of much of its information processing infrastructure, as well as paralysis in most vital industries. This would greatly reduce the capability of the target nation to conduct military operations of any substantial intensity.

Because conventional electromagnetic weapons produce negligible collateral damage, in comparison with conventional explosive munitions, they allow the conduct of an effective and high tempo campaign without the loss of life which is typical of conventional campaigns. This will make the option of a strategic bombing campaign more attractive to a Western democracy, where mass media coverage of the results of conventional strategic strike operations will adversely affect domestic civilian morale.

The long term effects of a sustained and concentrated strategic bombing campaign using a combination of conventional and electromagnetic weapons will be important. The cost of computer and communications infrastructure is substantial, and its massed destruction would be a major economic burden for any industrialised nation. In addition it is likely that poor protection of stored data will add to further economic losses, as much data will be lost with the destroyed machines.

From the perspective of conducting an IW campaign, this method of attack achieves many of the central objectives sought. Importantly, the massed application of electromagnetic weapons would inflict attrition on an opponent's information processing infrastructure very rapidly, and this would arguably add a further psychological dimension to the potency of the attack. Unlike the classical IW model of Gibsonian CyberWar, in which the opponent can arguably isolate his infrastructure from hostile penetration, parallel or hyperwar style massed attack with electromagnetic bombs will be be extremely difficult to defend against.

10.3. Offensive Counter Air (OCA) Operations using Electromagnetic Bombs

Electromagnetic bombs may be usefully applied to OCA operations. Modern aircraft are densely packed with electronics, and unless properly hardened, are highly vulnerable targets for electromagnetic weapons.

The cost of the onboard electronics represents a substantial fraction of the total cost of a modern military aircraft, and therefore stock levels of spares will in most instances be limited to what is deemed necessary to cover operational usage at some nominal sortie rate. Therefore electromagnetic damage could render aircraft unusable for substantial periods of time.

Attacking airfields with electromagnetic weapons will disable communications, air traffic control facilities, navigational aids and operational support equipment, if these items are not suitably electromagnetic hardened. Conventional blast hardening measures will not be effective, as electrical power and fixed communications cabling will carry electromagnetic induced transients into most buildings. Hardened aircraft shelters may provide some measure of protection due electrically conductive reinforcement embedded in the concrete, but conventional revetments will not.

Therefore OCA operations against airfields and aircraft on the ground should include the use of electromagnetic weapons as they offer the potential to substantially reduce hostile sortie rates.

10.4. Maritime Air Operations using Electromagnetic Bombs

As with modern military aircraft, naval surface combatants are fitted with a substantial volume of electronic equipment, performing similar functions in detecting and engaging targets and warning of attack. As such they are vulnerable to electromagnetic attack, if not suitably hardened. Should they be hardened, volumetric, weight and cost penalties will be incurred.

Conventional methods for attacking surface combatants involve the use of saturation attacks by anti-ship missiles or coordinated attacks using a combination of ARMs and anti-ship missiles. The latter instance is where disabling the target electronically by stripping its antennae precedes lethal attack with specialised anti-ship weapons.

An electromagnetic warhead detonated within lethal radius of a surface combatant will render its air defence system inoperable, as well as damaging other electronic equipment such as electronic countermeasures, electronic support measures and communications. This leaves the vessel undefended until these systems can be restored, which may or may not be possible on the high seas. Therefore launching an electromagnetic glidebomb on to a surface combatant, and then reducing it with laser or television guided weapons is an alternate strategy for dealing with such targets.

10.5. Battlefield Air Interdiction Operations using Electromagnetic Bombs

Modern land warfare doctrine emphasises mobility, and manoeuvre warfare methods are typical for contemporary land warfare. Coordination and control are essential to the successful conduct of manoeuvre operations, and this provides another opportunity to apply electromagnetic weapons. Communications and command sites are key elements in the structure of such a land army, and these concentrate communications and computer equipment. Therefore they should be attacked with electromagnetic weapons, to disrupt the command and control of land operations.

Should concentrations of armoured vehicles be found, these are also profitable targets for electromagnetic attack, as their communications and fire control systems may be substantially damaged or disabled as a result. A useful tactic would be initial attack with electromagnetic weapons to create a maximum of confusion, followed by attack with conventional weapons to take advantage of the immediate situation.

10.6. Defensive Counter-Air (DCA) and Air Defence Operations using Electromagnetic Warheads

Providing that compact electromagnetic warheads can be built with useful lethality performance, then a number of other potential applications become viable. One is to equip an Air-Air Missile (AAM) with such a warhead. A weapon with datalink midcourse guidance, such as the AIM-120, could be used to break up inbound raids by causing soft or hard electrical kills in a formation (raid) of hostile aircraft. Should this be achieved, the defending fighter will have the advantage in any following engagement as the hostile aircraft may not be fully mission capable. Loss of air intercept or nav attack radar, EW equipment, mission computers, digital engine controls, communications and electronic flight controls, where fitted, could render the victim aircraft defenceless against attack with conventional missiles.

This paradigm may also be applied to air defence operations using area defence SAMs. Large SAMs such as the MIM-104 Patriot, RIM-66E/M and RIM-67A Standard, 5V55/48N6 (SA-10) and 9M82/9M83 (SA-12) could accommodate an electromagnetic warhead comparable in size to a bomb warhead. A SAM site subjected to jamming by inbound bombers could launch a first round under datalink control with an electromagnetic warhead to disable the bombers, and then follow with conventional rounds against targets which may not be able to defend themselves electronically. This has obvious implications for the electromagnetic hardness of combat aircraft systems.

10.7. A Strategy of Graduated Response

The introduction of non-nuclear electromagnetic bombs into the arsenal of a modern air force considerably broadens the options

for conducting strategic campaigns. Clearly such weapons are potent force multipliers in conducting a conventional war, particularly when applied to Electronic Combat, OCA and strategic air attack operations.

The massed use of such weapons would provide a decisive advantage to any nation with the capability to effectively target and deliver them. The qualitative advantage in capability so gained would provide a significant advantage even against a much stronger opponent not in the possession of this capability.

Electromagnetic weapons however open up less conventional alternatives for the conduct of a strategic campaign, which derive from their ability to inflict significant material damage without inflicting visible collateral damage and loss of life. Western governments have been traditionally reluctant to commit to strategic campaigns, as the expectation of a lengthy and costly battle, with mass media coverage of its highly visible results, will quickly produce domestic political pressure to cease the conflict.

An alternative is a Strategy of Graduated Response (SGR). In this strategy, an opponent who threatens escalation to a full scale war is preemptively attacked with electromagnetic weapons, to gain command of the electromagnetic spectrum and command of the air. Selective attacks with electromagnetic weapons may then be applied against chosen strategic targets, to force concession. Should these fail to produce results, more targets may be disabled by electromagnetic attack. Escalation would be sustained and graduated, to produce steadily increasing pressure to concede the dispute. Air and sea blockade are complementary means via which pressure may be applied.

Because electromagnetic weapons can cause damage on a large scale very quickly, the rate at which damage can be inflicted can be very rapid, in which respect such a campaign will differ from the conventional, where the rate at which damage is inflicted is limited by the usable sortie rate of strategic air attack capable assets [15].

Should blockade and the total disabling of vital economic assets fail to yield results, these may then be systematically reduced by conventional weapons, to further escalate the pressure. Finally, a full scale conventional strategic air attack campaign would follow, to wholly destroy the hostile nation's warfighting capability.

Another situation where electromagnetic bombs may find useful application is in dealing with governments which actively implement a policy of state sponsored terrorism or info-terrorism, or alternately choose to conduct a sustained low intensity land warfare campaign. Again the Strategy of Graduated Response, using electromagnetic bombs in the initial phases, would place the government under significant pressure to concede.

Importantly, high value targets such as R&D and production sites for Weapons of Mass Destruction (nuclear, biological, chemical) and many vital economic sites, such as petrochemical production facilities, are critically dependent upon high technology electronic equipment. The proliferation of WMD into developing nations has been greatly assisted by the availability of high quality test and measurement equipment commercially available from First World nations, as well as modern electronic process control equipment. Selectively destroying such equipment can not only paralyse R&D effort, but also significantly impair revenue generating production effort. A Middle Eastern nation sponsoring terrorism will use oil revenue to support such activity. Crippling its primary source of revenue without widespread environmental pollution may be an effective and politically acceptable punitive measure.

As a punitive weapon electromagnetic devices are attractive for dealing with belligerent governments. Substantial economic, military and political damage may be inflicted with a modest commitment of resources by their users, and without politically damaging loss of life.

11. Conclusions

Electromagnetic bombs are Weapons of Electrical Mass Destruction with applications across a broad spectrum of targets, spanning both the strategic and tactical. As such their use offers a very high payoff in attacking the fundamental information processing and communication facilities of a target system. The massed application of these weapons will produce substantial paralysis in any target system, thus providing a decisive advantage in the conduct of Electronic Combat, Offensive Counter Air and Strategic Air Attack.

Because E-bombs can cause hard electrical kills over larger areas than conventional explosive weapons of similar mass, they offer substantial economies in force size for a given level of inflicted damage, and are thus a potent force multiplier for appropriate target sets.

The non-lethal nature of electromagnetic weapons makes their use far less politically damaging than that of conventional munitions, and therefore broadens the range of military options available.

This paper has included a discussion of the technical, operational and targeting aspects of using such weapons, as no historical experience exists as yet upon which to build a doctrinal model. The immaturity of this weapons technology limits the scope of this discussion, and many potential areas of application have intentionally not been discussed. The ongoing technological evolution of this family of weapons will clarify the relationship between weapon size and lethality, thus producing further applications and areas for study.

E-bombs can be an affordable force multiplier for military forces which are under post Cold War pressures to reduce force sizes, increasing both their combat potential and political utility in resolving disputes. Given the potentially high payoff deriving from the use of these devices, it is incumbent upon such military forces to appreciate both the offensive and defensive implications of this technology. It is also incumbent upon governments and private industry to consider the implications of the proliferation of this

technology, and take measures to safeguard their vital assets from possible future attack. Those who choose not to may become losers in any future wars.

12. Acknowledgements

Thanks to Dr D.H. Steven for his insightful comment on microwave coupling and propagation, and to Professor C.S. Wallace, Dr Ronald Pose and Dr Peter Leigh-Jones for their most helpful critique of the drafts. Thanks also to the RAAF Air Power Studies Centre and its then Director, Group Captain Gary Waters, for encouraging the author to investigate this subject in 1993. Some material in this paper is derived from RAAF APSC Working Paper 15, "A Doctrine for the Use of Electromagnetic Pulse Bombs", published in 1993 [KOPP93], and is posted with permission.

An earlier version of this paper was presented at InfoWarCon V and first published in "Information Warfare - Cyberterrorism: Protecting Your Personal Security In the Electronic Age", 1996, Thunder's Mouth Press, 632 Broadway 7th FL, New York, NY, ISBN: 1-56025-132-8, http://www.infowar.com, posted with permission.

13. References

AAP1000 - RAAF, DI(AF) AAP1000, The Air Power Manual, Second Edition, RAAF APSC, Canberra, 1994

AAP1003 - RAAF, DI(AF) AAP1003, Ch.8 The Law of Aerial Targeting, Operations Law for RAAF Commanders, First Edition, RAAF APSC, Canberra, 1994

AFM1-1 - Basic Aerospace Doctrine of the United States Air Force, Air Force Manual 1-1, Volume 1, March 1992.

CAIRD85 - Caird R.S. et al, Tests of an Explosive Driven Coaxial Generator, Digest of Technical Papers, 5th IEEE Pulsed Power Conference, pp.220, IEEE, New York, 1985.

DIXON84 - Dixon R.C., Spread Spectrum Systems, John Wiley and Sons, New York, 1984.

FANTHOME89 - Fanthome B.A., MHD Pulsed Power Generation, Digest of Technical Papers, 7th IEEE Pulsed Power Conference, pp.483, IEEE, New York, 1989.

FLANAGAN81 - Flanagan J., High-Performance MHD Solid Gas Generator, Naval Research Lab, Patent Application 4269637, May 1981.

FOWLER60 - C. M. Fowler, W. B. Garn, and R. S. Caird, Production of Very High Magnetic Fields by Implosion, Journal of Applied Physics, Vol. 31, No. 3, 588-594, March, 1960.

FOWLER89 - C. M. Fowler,R. S. Caird, The Mark IX Generator, Digest of Technical Papers, Seventh IEEE Pulsed Power Conference, 475, IEEE, New York, 1989.

FULGHUM93 - Fulghum, D.A., ALCMs Given Non Lethal Role, Aviation Week & Space Technology, February 22, 1993.

GLASSTONE64 - S. Glasstone, Editor, The Effects of Nuclear Weapons, US AEC, April, 1962, Revised Edition February, 1964.

GOFORTH89 - Goforth J.H. et al, Experiments with Explosively Formed Fuse Opening Switches in Higher Efficiency Circuits, Digest of Technical Papers, 7th IEEE Pulsed Power Conference, pp.479, IEEE, New York, 1989.

GRANATSTEIN87 - Granatstein V.L., Alexeff I., High Power Microwave Sources, Artech House, Boston, London, 1987

HERSKOVITZ96 - Herskowitz D., The Other SIGINT/ELINT, Journal of Electronic Defence, April, 1996.

HOEBERLING92 - Heoberling R.F., Fazio M.V., Advances in Virtual Cathode Microwave Sources, IEEE Transactions on Electromagnetic Compatibility, Vol. 34, No. 3, 252, August 1992.

ICH10 - EW Systems: AN/ Designated Hardware, pp.86, International Countermeasures Handbook, 10th Edition, Cardiff Publishing, Colorado, 1985.

ICH14 - International Countermeasures Handbook, 14th Edition, Cardiff Publishing, Colorado, 1989.

JED95 - USAF Looks for HPM SEAD Solution, pp.36, Journal of Electronic Defence, September, 1995.

JED96 - Hughes to Build HPM SEAD Demonstrator, pp.29, Journal of Electronic Defence, February, 1996.

KIRTLAND94 - High Energy Microwave Laboratory, Fact Sheet, USAF AFMC, Phillips Laboratory, Kirtland AFB, 1994.

KOPP92 - Kopp C., Command of the Electromagnetic Spectrum - An Electronic Combat Doctrine for the RAAF, Working Paper No.8, Air Power Studies Centre, Royal Australian Air Force, Canberra, November 1992.

KOPP93 - Kopp C., A Doctrine for the Use of Electromagnetic Pulse Bombs, Working Paper No.15, Air Power Studies Centre, Royal Australian Air Force, Canberra, July 1993.

KOPP96 - Kopp C., Australia's Kerkanya Based Agile Gliding Weapon, pp.28, Australian Aviation, Aerospace Publications, Canberra, June 1996.

KRAUS88 - Kraus J.D., Antennas, Second Edition, McGraw-Hill, 1988.

MDC95 - Joint Direct Attack Munition (JDAM), unclassified briefing, McDonnell Douglas Corporation, 1995, unpublished material.

MICRON92 - Micron DRAM Data Book, Micron Technology Inc, Idaho, 1992.

MOTO3 - Motorola RF Device Data, Motorola Semiconductor Products Inc, Arizona, 1983.

NATSEMI78 - CMOS Databook, National Semiconductor Corporation, Santa Clara, 1978

NORTHROP95 - B-2 Precision Weapons, unclassified briefing, Northrop-Grumman Corporation, September, 1995, unpublished material.

NPI93 - NPI Local Area Network Products, SMD Transformers, Nano Pulse Industries, Brea, 1993.

PERGLER94 - Pergler R., Joint Standoff Weapon System (JSOW), unclassified briefing, Texas Instruments, Inc., December 1994, unpublished material.

RAMO65 - Ramo S. et al, Fields and Waves in Communications Electronics, New York, John Wiley & Sons, 1965

REINOVSKY85 - Reinovsky R.E., Levi P.S. and Welby J.M., An Economical, 2 Stage Flux Compression Generator System, Digest of Technical Papers, 5th IEEE Pulsed Power Conference, pp.216, IEEE, New York, 1985.

SANDER86 - Sander K. F. and G.A.L. Reed, Transmission and Propagation of Electromagnetic Waves, Cambridge University Press, 1986.

STAINES93 - Staines, G.W., High Power Microwave Technology - Part IV, Military Applications of High Power Microwaves, Salisbury, DSTO ERL, EWD, 1993, draft paper.

SZAFRANSKI95 - Szafranski R., Col USAF, Parallel War and Hyperwar, Chapter 5 in Schneider B.R, Grinter L.E., Battlefield of the Future, 21st Century Warfare Issues, Air University Press, Maxwell AFB, September 1995.

TAYLOR92 - Taylor C.D., Harrison C.W., On the Coupling of Microwave Radiation to Wire Structures, IEEE Transactions on Electromagnetic Compatibility, Vol. 34, No. 3, 183, August 1992.

THODE87 - Thode L.E., Virtual-Cathode Microwave Device Research: Experiment and Simulation, Chapter 14 in High Power Microwave Sources, 1987.

VECK85 - van Eck W., "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk", Computers and Security, 1985, pp. 269.

WARDEN95 - Warden J.A. III, Col USAF, Air Theory for the Twenty-first Century, Chapter 4 in Schneider B.R, Grinter L.E., Battlefield of the Future, 21st Century Warfare Issues, Air University Press, Maxwell AFB, September 1995.

WATERS92 - Waters Gary, Gulf Lesson One, Canberra, Air Power Studies Centre, 1992

WHITE78 - The EMP - A Triangular Impulse, 2.29, A Handbook Series on Electromagnetic Interference and Compatibility, Don White Consultants, Maryland, 1978.

Carlo Kopp Born in Perth, Western Australia, the author graduated with first class honours in Electrical Engineering in 1984, from the University of Western Australia. In 1996 he completed an MSc in Computer Science and is currently working on a PhD in the same discipline, at Monash University in Melbourne, Australia. He has over a decade of diverse industry experience, including the design of high speed communications equipment, optical fibre receivers and transmitters, communications equipment including embedded code, Unix computer workstation motherboards, graphics adaptors and chassis. More recently, he has consulted in Unix systems programming, performance engineering and system administration. Actively publishing as a defence analyst in Australia's leading aviation trade journal, Australian Aviation, since 1980, he has become a locally recognised authority on the application of modern military technology to operations and strategy. His work on electronic combat doctrine, electromagnetic weapons doctrine, laser remote sensing and signature reduction has been published by the Royal Australian Air Force's Air Power Studies Centre since 1992, and he has previously contributed to CADRE Air Chronicles.

1 - Electromagnetic pulse or EMP device is a generic term applied to any device, nuclear or conventional, which is capable of generating a very intense but short electromagnetic field transient. For weapons applications, this transient must be sufficiently intense to produce electromagnetic power densities which are lethal to electronic and electrical equipment. Electromagnetic weapons are electromagnetic devices specifically designed as weapons. Whilst the terms 'conventional EMP weapon' and 'High

Power Microwave or HPM weapon' have been used interchangeably in trade journals (see FULGHUM93), this paper will distinguish between microwave band and low frequency weapons. The term 'electromagnetic bomb' or 'E-bomb' will be used to describe both microwave and low frequency non-nuclear bombs. This paper will not address the use of nuclear EMP, or alternate uses of HPM technology. HPM technology has a broad range of potential applications in EW, radar and directed energy weapons (DEW). The general conclusions of this paper in the areas of infrastructure vulnerability and hardening are also true for microwave directed energy weapons. This paper extends the scope of earlier work by the author on this subject [KOPP93].

2 - One bizzare instance of lightning strike electrical damage was described to the author by an eyewitness technician, tasked with assessing the damage on the site. A lightning bolt impacted in the close vicinity of a transmitter shed. RF and power cables ran from the transmitter shed to a transmission tower through a rectangular, metal shielded tunnel. The effect of the lightning strike was to produce an electromagnetic standing wave in the tunnel, much like in a microwave waveguide. All cables within the tunnel were burned through at regular spacings along the tunnel, corresponding precisely to the half wavelength of the standing wave in the tunnel.

3 - The NACSIM 5100A standard specifies acceptable emission levels for TEMPEST (Transient ElectroMagnetic Pulse Emanation Standard) rated equipment.

4 - The Northrop/Lockheed ASD-5 Black Crow DF receiver was fitted to the AC-130A Pave Pronto gunships, rebuilt from obsoleted C-130 transports [ICH10].

5 - A noteworthy technical issue in this context is that even equipment not-rated to TEMPEST standards will radiate energy at very low power levels, in comparison with intentional transmissions by radar or communications equipment. A receiver designed to detect, identify and locate sources of UE radiation will either need to be highly sensitive, or deployed very close to the emitter. It is worth noting that UE from computer monitors and networks exhibit known regular patterns, and correlation techniques could be used to significantly improve receiver sensitivity [DIXON84].

6 - Fulghum D.A., ALCMs Given Non Lethal Role, AW&ST, Feb 22, 1993. This recent report indicates that the US has progressed significantly with its development work on electromagnetic warhead technology. An electromagnetic warhead was fitted to the USAF AGM-86 Air Launched Cruise Missile airframe, involving both structural and guidance system modifications. The description in this report suggests the use of an explosive pumped flux generator feeding a device such as a Vircator. References to magnetic coils almost certainly relate to the flux compression generator hardware.

7 - The Journal of Electronic Defence [JED96] recently reported on the USAF Phillips Laboratory at Kirtland awarding a $6.6M HPM SEAD weapon technology demonstration program contract to Hughes Missile Systems Co. This contract will see Hughes conduct design studies in order to define design goals, and then fabricate brassboard demonstration hardware using government developed technology. JED speculate that the weapon will be a FCG driven microwave tube, which is most likely the case given the USAF's prior research activities in this area [REINOVSKY85]. An earlier report [JED95] indicated the existence of a related program which addresses command and control warfare and counter-air capabilities. In any event, the devices produced by these programs are likely to become the first operationally fielded HPM electromagnetic bombs for delivery by combat aircraft.

8 - This may be readily determined by calculating the ratio of warhead mass to total weapon launch mass, for representative missile types. Taking the AGM-78 Standard as a lower limit yields 15.9%, whereas taking the AGM/BGM-109 Tomahawk as an upper limit yields about 28%. Figures are derived from manufacturers' brochures and reference publications eg Jane's Air-Launched Weapons.

9 - Staines, Fulghum. This is entirely consistent with theoretical expectations, as the different spectral characteristics of microwave electromagnetic warheads, compared to nuclear electromagnetic weapons, will significantly affect the effectiveness of protective filters. What is important from an electrical engineering viewpoint is that a filter designed to stop signals in the lower frequency bands may perform very poorly at microwave frequencies.

10 - See International Countermeasures Handbook, 14th Edition, pp 104.

11 - Gary Waters, Gulf Lesson One. Chapter 16 of this reference provides a good discussion of both the rationale and implementation of this strategy.

12 - Soft kill means will inhibit or degrade the function of a target system during their application, leaving the target system electrically and physically intact upon the cessation of their application. Hard kill means will damage or destroy the target system, and are thus a means of inflicting attrition.

13 - This is also the stated intent of the USAF HPM SEAD technology demonstration program. The fact that the first application of a HPM bomb is electronic combat underscores the tactical, operational and strategic importance of first defeating an air defence system when prosecuting a strategic air war.

14 - The classical argument here is centred upon Allied experience in bombing Germany during WW2, where even repeated raids on industrial targets were unable to wholly stop production, and in many instances only served to reduce the rate of increase in production. What must not be overlooked is that both the accuracy and lethality of weapons in this period bore little comparison to what is available today, and automation of production facilities was almost non-existent.

15- This constraint primarily results from limitations in numbers. Strategic air attack requires precision delivery of substantial payloads, and is thus most effectively performed with specialised bomber assets, such as the B-52, B-1, B-2, F-111, F-15E, F-

117A, Tornado or Su-24. These are typically more maintenance intensive than less complex multirole fighters, and this will become a constraint to the sortie rate achievable with a finite number of aircraft, assuming the availability of aircrew. Whilst multirole fighters may be applied to strategic air attack, their typically lesser payload radius performance and lesser accuracy will reduce their effectiveness. In the doctrinal context, this can be directly related to existing USAF aerospace doctrine [AFM1-1], in several areas.

A version of this article was first published in: "Information Warfare - Cyberterroism: Protecting Your Personal Security in the Electronic Age" by Winn Schwartau, 1996 Thunder's Mouth Press, 632 Broadway 7th Fl, New York, New York, ISBN: 1-56025-132-8, http://www.infowar.com