

Electro Magnetic Pulse

The Danger You Never Hear About

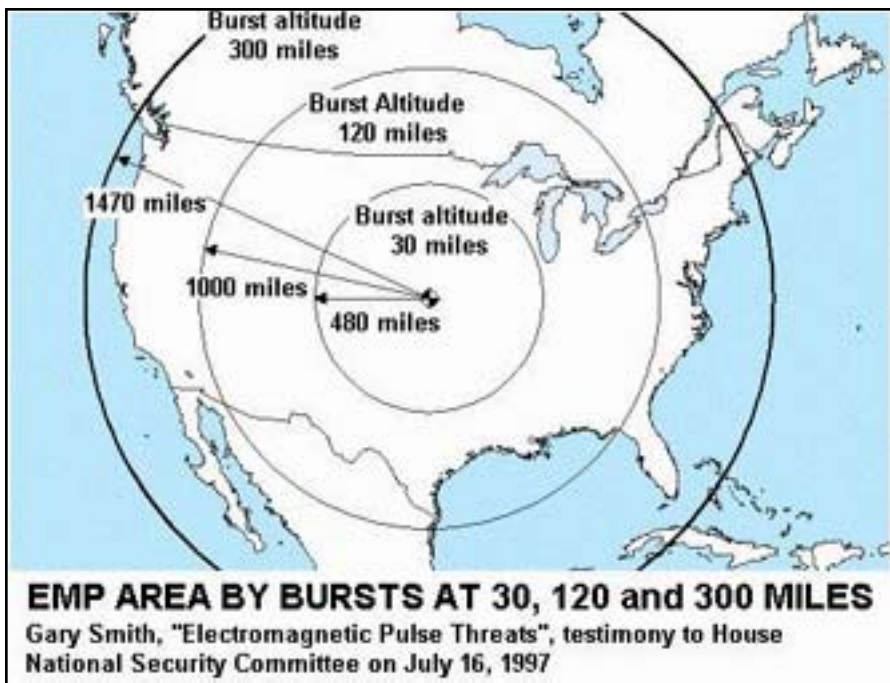
“Russia is among the best in the world when it comes to manufacturing this type of electronic weapon,” said Anders Kallenaas of the Swedish National Defense’s Research Institute (FOA).

Quoting the Swedish newspaper Svenska Dagbladet (1-23-98), the news agency AFP said the high-power microwave bombs (“bear cans”) could be bought on the Russian market for “several hundreds of thousands kronor” (< \$150,000) and had already been bought by the Australian military among others.

It said the bomb was stored in a briefcase and emitted short, high-energy pulses reaching 10 gigawatts, which could destroy complex electronics systems. As tested, the bomb presents a threat to the Swedish military, in particular to the JAS 39 Gripen jet fighter that it is trying to export. It can, also, knock out electronic systems of nuclear or electric power plants, banks, trains, or even a simple telephone switchboard.

Despite the science-fiction flavor, the electro-magnetic bomb is close to reality. It has been the subject of extensive research in the US and presumably (Sakharov tested his magnetic compression generator 40 years ago + Altshuler, Voitenko and Bichenkov) Russia for decades. The concept arose through early nuclear testing, when scientists realized that high altitude atomic blasts produced an electro-magnetic pulse capable of destroying delicate electronics systems on the ground.

Any thermonuclear war would have started with such ionospheric blasts. One consequence was that military computer and electronic systems were “hardened” to minimize such damage, but civil systems remain vulnerable. Two types of non-nuclear EMP devices have been developed. One uses conventional explosives to induce the EMP; another uses a single-use, high-power microwave generation device.



EMP capabilities were discussed in a paper published by the RAAF Air Power Studies Center in 1996. Its author, defense analyst Carlo Copp, [1] concluded that the design and deployment of electro-magnetic warheads for bombs and missiles was technically feasible in the next decade. “Providing that satisfactory solutions can be found for these problems, electro-magnetic munitions for bomb and missile applications promise to be an important and robust weapon in both strategic and tactical operations, offering significantly reduced collateral damage and lower human casualties than established weapons,” he said.

“High Power Electro-magnetic Pulse generation techniques and High Power Microwave technology have matured to the point where practical E-bombs (Electro-magnetic 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 doc-

trinal foundation for the use of such devices in warhead and bomb applications.”

It can be used by special forces teams who infiltrate the enemy’s and detonate a device near their electronic devices. It destroys the electronics of all computer and communication systems in a quite large area. The EMP bomb can be smaller than a HERF gun to cause a similar amount of damage and is typically-used to damage not a single target (not aiming in one direction) but to damage all equipment near the bomb. [2]

The efficient execution of an Information Warfare campaign against a modern industrial or post-industrial opponent will require the use of specialized tools designed to destroy information systems. High Power Electro-magnetic Pulse generation techniques and High Power Microwave technology have matured to the point where practical electro-magnetic bombs are becoming technically feasible, with new applications in both Strategic and Tactical IW (Information Warfare).

Targets of the E-bombs:

The telecommunication systems
The national power grid
Finance and banking systems
The national transporting systems
The mass media
Because these systems based on electronic systems.

A Radio Frequency Weapon is one that uses intense pulses of RF energy to destroy or degrade the electronics in a target. These weapons can be employed in a narrow beam over a long distance to a point target. They are categorized as High Power Microwave Weapons (HPM) and Ultra Wide Band Weapon (UWB). The phrase non-nuclear electro-magnetic pulse is sometimes used.

Advantages of the HPM:

All weather
Low cost per engagement
Possible to engage multiple targets
Non-lethal to humans
Not able to detect attacks

Electro-magnetic effects

The high temperatures and energetic radiation produced by nuclear explosions also produce large amounts of ionized (electrically charged) matter which is present immediately after the explosion. Under the right conditions, intense currents and electro-magnetic fields can be produced, generically called EMP (Electro-magnetic Pulse), that are felt at long distances. Living organisms are impervious to these effects, but electrical and electronic equipment can be temporarily or permanently disabled by them. Ionized gases can, also, block short wavelength radio and radar signals (fireball blackout) for extended periods.

The occurrence of EMP is strongly dependent on the altitude of burst. It can be significant for surface or low altitude bursts (below 4,000 m); it is very significant for high altitude bursts (above 30,000 m); but it is not significant for altitudes between these extremes. This is because EMP is generated by the asymmetric absorption of instantaneous gamma rays produced by the explosion. At intermediate altitudes the air absorbs

these rays fairly uniformly and does not generate long range electro-magnetic disturbances.



The formation EMP begins with the very intense, but very short burst of gamma rays caused by the nuclear reactions in the bomb. About 0.3% of the bomb's energy is in this pulse, but it lasts for only 10 nanoseconds or so. These gamma rays collide with electrons in air molecules, and eject the electrons at high energies through a process called Compton scattering. These energetic electrons in turn knock other electrons loose, and create a cascade effect that produces some 30,000 electrons for every original gamma ray.

In low altitude explosions the electrons, being very light, move much more quickly than the ionized atoms from which they are removed, and diffuse away from the region where they are formed. This creates a very strong electric field which peaks in intensity to 10 nanoseconds. The gamma rays emitted downward, however, are absorbed by the ground which prevents charge separation from occurring. This creates a very strong vertical electric current which generates intense electro-magnetic emissions over a wide frequency range (up to 100 MHz) that emanate mostly horizontally. At the same time, the earth acts as a conductor allowing the electrons to flow back toward the burst point, where the positive ions are concentrated. This produces a strong magnetic field along the ground. Although only about 3×10^{-10} of the total explosion energy is radiated as EMP in a ground burst (10-6 joules for 1 Mt bomb), it is concentrated in a very short pulse. The charge separation persists for only a few tens of microseconds, making the emission power some 100 gigawatts. The field strengths for

ground bursts are high only in the immediate vicinity of the explosion. For smaller bombs they aren't very important because they are strong only where the destruction is intense anyway. With increasing yields, they reach farther from the zone of intense destruction. With a 1 Mt bomb, they remain significant out to the 2 psi overpressure zone (5 miles).

High altitude explosions produce EMPs that dramatically more destructive. About 3×10^{-5} of the bomb's total energy goes into EMP in this case, 10^{11} joules for a 1 Mt bomb. EMP is formed in high altitude explosions when the downwardly directed gamma rays encounter denser layers of air below. A pancake shaped ionization region is formed below the bomb. The zone can extend all the way to the horizon, to 2500 km for an explosion at an altitude of 500 km. The ionization zone is up to 80 km thick at the center. The Earth's magnetic field causes the electrons in this layer to spiral as they travel, creating a powerful downward directed electro-magnetic pulse lasting a few microseconds. A strong vertical electrical field (20-50 KV/m) is also generated between the Earth's surface and the ionized layer, this field lasts for several minutes until the electrons are recaptured by the air. Although the peak EMP field strengths from high altitude bursts are only 1-10% as intense as the peak ground burst fields, they are nearly constant over the entire Earth's surface under the ionized region.

The effects of these field on electronics is difficult to predict, but can be profound. Enormous induced electric currents are generated in wires, antennas, and metal objects (like missiles, airplanes, and building frames). Commercial electrical grids are immense EMP antennas and would be subjected to voltage surges far exceeding those created by lightning, and over vastly greater areas. Modern VLSI chips are extremely sensitive to voltage surges, and would be burned out by even small leakage currents. Military equipment is generally designed to be resistant to EMP, but realistic tests are very difficult to perform and EMP protection rests on attention to detail. Minor changes in design, incorrect mainte-

nance procedures, poorly fitting parts, loose debris, moisture, and ordinary dirt can all cause elaborate EMP protections to be totally circumvented. It can be expected that a single high yield, high altitude explosion over an industrialized area would cause massive disruption for an indeterminable period, and would cause huge economic damages (all those damaged chips add up).

A separate effect is the ability of the ionized fireball to block radio and radar signals. Like EMP, this effect becomes important with high altitude bursts. Fireball blackout can cause radar to be blocked for tens of seconds to minutes over an area tens of kilometers across. High frequency radio can be disrupted over hundreds to thousands of kilometers for minutes to hours depending on exact conditions.

The technology base for E-bombs

Explosively Pumped Flux Compression Generators (FCG)

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 as a high voltage capacitor bank (Marx bank), a smaller FCG or the MHD device. A number of geometrical configurations for FCGs have been published. 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. In principle, any device capable of producing a pulse of electrical current of the order of tens of KiloAmperes to MegaAmperes will be suitable.

Explosive and Propellant driven MHD Generators

The fundamental principle behind the design of MHD devices is that a conductor moving through a magnetic field will produce an electrical current trans-

verse to the direction of the field and the conductor motion. In an explosive or propellant driven MHD device, the conductor is a plasma of ionized explosive or propellant gas, which travels through the magnetic field. Current is collected by electrodes, which are in contact with the plasma jet. The electrical properties of the plasma are optimized by seeding the explosive or propellant with suitable additives, which ionize during the burn.

High Power Microwave Sources (Vircator)

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.

Coupling modes

The 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.

Front door coupling occurs typically when power from an electro-magnetic 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.

Back Door Coupling occurs when the electro-magnetic field from a weapon produces large transient currents 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.

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. While 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.

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.

The importance of glide-bombs as delivery means for HPM warheads is threefold. Firstly, the glide-bomb can be released from outside effective radius of target air defenses, therefore minimizing 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.

Targeting Electro-magnetic Bombs

The task of identifying targets for attack with electro-magnetic 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 electro-magnetic bomb can be programmed to detonate at the optimal position to inflict a maximum of electrical damage.

Mobile and camouflaged targets, which radiate overtly, can also be readily-engaged. Mobile and relocatable air defense 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-data-linked to the launch platform. As most such targets move relatively slowly, they are unlikely to escape the footprint of the electro-magnetic 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). UE has attracted most attention in the context of TEMPEST 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, such emissions can only be suppressed by rigorous shielding and emission control techniques, such as are employed in TEMPEST rated equipment.

While the demodulation of UE can be a technically-difficult task to perform well, in the context of targeting electro-magnetic 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, switch-mode power supplies, electrical motors, internal combustion engine ignition systems, variable duty cycle electrical power controllers (thyristor or triac based), super-heterodyne 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 inter-diction gun-ships which used direction finding receivers to track the emissions from vehicle ignition systems. Once a truck was identified and

tracked, the gun-ship would engage it.

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 over-fly hostile territory to find signals of usable intensity. 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 electro-magnetic 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.

Defense against E-bombs

The most effective defense against electro-magnetic 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 electro-magnetic weapons effects must be electro-magnetically-hardened.

The most effective method is to wholly contain the equipment in an electrically conductive enclosure, termed a Faraday cage, which prevents the electro-magnetic 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 fibers address this requirement for transferring data in and out, electrical power feeds remain an ongoing vulnerability.

Where an electrically conductive channel must enter the enclosure, electro-magnetic 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 electro-magnetic devices. Reports from the US indicate that hardening measures attuned to the behavior of nuclear EMP bombs do

not perform well when dealing with some conventional microwave electro-magnetic device designs.

It is significant that hardening of systems must be carried out at a system level, as electro-magnetic 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.

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 electro-magnetic 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 (i.e.. spread spectrum) techniques should be employed exclusively to preclude the use of site emissions for electro-magnetic targeting purposes. 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 electro-magnetic 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.

Virtual prototyping of RF weapons

Complex and expensive experimental efforts are more timely and cost-effective if they are tested by theoretical and computational modeling. Such computations are made tractable by viewing the device as a system consisting of a pulsed power source, microwave source, and an antenna.

Electro-magnetic bombs are Weapons of Electronical 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.

Conclusions

Electro-magnetic bombs are Weapons of Electronical 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 article 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.

Pearl Harbor — 9-11 — EMP!

What a perfect way to get the American Sheeple to back another war. It has worked before, so why not again? Just make it look like Iran or, as in Pearl Harbor, allow the enemy to do it for you. Americans, who at the present time have a belly full of war on foreign lands, would fully-support Barry Soetoro and our evil government waging yet another war, killing millions of innocent victims.

The Remnant need to be aware of where all the chessmen are on the board and remain alert to to the possible plays that can be used, as before, to align them into doing the predictable.

Think — prepare — survive!

